CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-17 Medicare Business Partners Systems Security	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 9	**Date: June 20, 2008**
	Change Request 5976

Subject: CMS Business Partner Systems Security Manual

I. SUMMARY OF CHANGES: The BPSSM was updated to reflect changes in NIST, OMB and HHS requirements.

New / Revised Material
Effective Date: July 1, 2008
Implementation Date: July 22, 2008

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	Chapter / Section / Subsection / Title
R	Record of Changes
R	Table of Contents
R	1/Introduction
R	1.1/Additional Requirements for MAC Contractors
R	2/IT Systems Security Roles and Responsibilities
R	2.1/CMS Project Officer (PO)
R	2.2/The (Principal)Systems Security Officer (SSO)
R	2.3/Business Owners
R	2.4/System Maintainers/Developers
R	2.5/Personnel Security/Suitability
R	3/IT Systems Security Program Management
R	3.1/System Security Plan (SSP)
R	3.2/Risk Assessment
R	3.3/Certification
R	3.4/Information Technology (IT) Systems Contingency Plan

R	3.5.2/Annual FISMA Evaluation (FE)
D	3.5.2.1/Background
D	3.5.2.2/POAandM Package Components/Submission Format
R	3.5.3/Plan of Action and Milestones (POAandMs)
N	3.5.3.1/Background
N	3.5.3.2/POAandM Package Components/Submission Format
N	3.5.4/Annual/Yearly Compliance Condition
R	3.6/Incident Reporting and Response
R	3.6.1/Computer Security Incident Response
R	3.7/System Security Profile
R	3.10.1/Security Configuration Management
R	3.10.2/National Institute of Standards and Technology (NIST)
R	4.1/Security Objectives
R	4.1.1/Potential Security Impact Levels
R	4.1.2/Security Levels by Information Type
R	4.1.3/CMS Security Level Designation-HIGH
N	4.1.4/Minimum System Security Requirements-HIGH
R	4.2/Sensitive Information Protection Requirements
R	4.2.1/Restricted Area
R	4.2.2/Security Room
R	4.2.3/Secured Areas (Secured Interior / Secured Perimeter)
R	4.2/4.2.4/Containers
R	4.2.4.1/Locked Container
R	4.2.4.2/Security Container
R	4.2.4.3/Safes/Vaults
R	4.2.5/Locking Systems
R	4.2.6/Intrusion Detection Systems (IDS)
R	5/Internet Security
R	Appendix A/The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs)
D	Appendix A/Attachment A/ CMS CSRs
N	Appendix A/Attachment 1/CMS Core Security Requirements (CSR) for High Impact Level Assessments

N	Appendix A/Attachment 2/CMS Core Security Requirements (CSR) for Moderate Impact Level Assessments
N	Appendix A/Attachment 3/CMS Core Security Requirements (CSR) for Low Impact Level Assessments
R	Appendix B/Medicare Information Technology (IT) Systems Contingency Planning
R	Appendix D/CMS Information Security (IS) Guidebook for Audits
R	Appendix E/CMS Guidelines
R	Appendix F/Security Configuration Management
R	Appendix G/Acronyms and Abbreviations
R	Appendix H/Glossary

III. FUNDING:
SECTION A: For Fiscal Intermediaries and Carriers:
No additional funding will be provided by CMS; Contractor activities are to be carried out within their operating budgets.

SECTION B: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:

Business Requirements

Manual Instruction

**Unless otherwise specified, the effective date is the date of service.*

Attachment – Business Requirements

Pub. 100-17	Transmittal: 9	Date: June 20, 2008	Change Request: CR 5976

SUBJECT: Business Partners Systems Security Manual

Effective Date: **July 1, 2008**

Implementation Date: July 22, 2008

I. GENERAL INFORMATION

A. Background: The purpose of this updates is to communicate to Medicare Contractors changes to CMS requirements and to incorporate the revision of NIST SP 800-53 as well as OMB mandates. Additionally, the CSRs were updated to reflect the latest changes to NIST SP 800-53 and NIST SP 800-53A.

B. Policy: The policy (s) mandating this change request are the Federal Information Security Management Act of 2002, National Institute of Standards and Technology guidance, and CMS policies, standards, guidelines and procedures.

II. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement

Number	Requirement	Responsibility (place an "X" in each applicable column)									
		A/B MAC	DME MAC	FI	CARRIER	RHHI	Shared-System Maintainers				Other
							FISS	MCS	VMS	CWF	
5976.1	Medicare Contractors shall follow the processes outlined in the Medicare Business Partners Systems Security Manual.	X	X	X	X	X	X	X	X	X	X (HIGLAS, EDCs & PSCs)
5976.2	Medicare Contractors shall follow the instructions and guidance when evaluating all CSRs and preparing CSR responses.	X	X	X	X	X	X	X	X	X	X (HIGLAS, EDCs & PSCs)

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility (place an "X" in each applicable column)									
		A/B MAC	DME MAC	FI	CARRIER	RHHI	Shared-System Maintainers				Other
							FISS	MCS	VMS	CWF	
	None.										

IV. SUPPORTING INFORMATION

Section A: For any recommendations and supporting information associated with listed requirements, use the box below: N/A
"Should" denotes a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: For all other recommendations and supporting information, use this space: N/A

V. CONTACTS

Pre-Implementation Contact(s): Kevin Potter 410.786.5686 and Sherwin Schulterbrandt 410.786.0743

Post-Implementation Contact(s): Kevin Potter 410.786.5686 and Sherwin Schulterbrandt 410.786.0743

VI. FUNDING

Section A: For *Fiscal Intermediaries (FIs), Carriers, and Regional Home Health Carriers (RHHIs)*:

No additional funding will be provided by CMS; contractor activities are to be carried out within their operating budgets.

Section B: *For Medicare Administrative Contractors (MACs)*:

The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

Centers for Medicare & Medicaid Services (CMS)

Business Partners

Systems Security Manual

CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

(Rev. 9, 06-20-08)

CMS/Business Partners
Systems Security Manual

Record of Changes

Revision	Major Changes	Date
9	*Main document and all appendices: Updated to reflect new FISMA Evaluation process and new CMS CSRs.* *1 – 1.1: Updated list of document references, titles, and links.* *2.1: Deleted all references to CCMO.* *2.2: Deleted reference to Line One funding.* *2.3: Changed System Owners/Managers to Business Owners.* *3: Changed Self-Assessment to FISMA Evaluation. Updated Table 3.1 from Self-Assessment to FISMA Evaluation and added and used acronyms where applicable; and added acronyms to Legend and contract type address list. Updated footnote titles. Deleted Consortia contact and address information and all CCMO references.* *3.1: Changed System Owners/Managers to Business Owners. Updated document titles and links.* *3.2: Updated document titles and links.* *3.3: Changed Self-Assessment to FISMA Evaluation.* *3.3: Clarified backup facility testing when multiple contract types are involved.* *3.4: Clarified annual testing requirement when multiple Medicare contracts are involved.* *3.5.2: Added Section 3.5.2, Annual FISMA Evaluation (FE) to explain new FISMA validation requirement.* *3.5.3 – 3.5.4: Updated section numbers and changed Self-Assessment to FISMA Evaluation.* *3.6: Updated Security Incident definition.*	*06/08*

Revision	Major Changes	Date
	3.6.1: Updated Security Incident response requirements. Added new Table 3.2, Incident Categories, and Table 3.3, Incident Reporting Timeframe Criteria. Updated reference to new CMS incident reporting procedures.	
	3.7: Changed CISS Self-Assessment to FISMA Evaluation.	
	3.10.2: Updated Table 3.4, NIST Publications.	
	4 – 4.1.4: Rewrote section 4.1 and all of its subsections to incorporate FIPS Pub 199 security categorization standards, potential security impact levels, security levels by information type, CMS security level designation—HIGH, and minimum system security requirements—HIGH. Added Table 4.1, System Security Level Definitions, and Table 4.2, FIPS 199 Security Levels by Information Type.	
	4.2 – 4.2.6: Revised sections to incorporate and clarify revised information protection requirements.	
	5: Added one exception to the CMS Internet policy allowing the submission of Form 1099 using the IRS FIRE system.	
	Appendix A: Rewrote most of this appendix to replace the former annual Self-Assessment with the new annual FISMA Evaluation requirement, the new CSR format, and their new response status reporting requirements. Completely rewrote the former CSRs and added separate CSR attachments for: (1) High Impact Level, (2) Moderate Impact Level, and (3) Low Impact Level Assessments.	
	Appendix B: Added information about the tabletop test and the CMS tabletop test procedures reference.	
	Appendix D: Clarified CFO/EDP audit information, changed Self-Assessment to FISMA Evaluation, and clarified some acronyms.	
	Appendix E: Clarified some acronyms, changed Self-Assessment to FISMA Evaluation, and updated some NIST references. Added new whitepapers to appendix.	
	Appendix F: Clarified some acronyms, and updated some references and their links. Added new section 4.0, HHS	

Revision	Major Changes	Date
	Federal Desktop Core Configuration (FDCC) Standard for Windows XP. *Appendix G: Added new acronyms.* *Appendix H: Added new terms and definitions, and updated some existing definitions.*	

CMS/Business Partners
Systems Security Manual

Table of Contents

(Rev. 9, 06-20-08)

Appendices

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Centers for Medicare & Medicaid Services (CMS) requires that its business partners implement information technology (IT) systems security controls in order to maintain the confidentiality, integrity, and availability of Medicare systems operations in the event of computer incidents or physical disasters.

A CMS business partner (contractor) is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Medicare carriers, Fiscal Intermediaries, Common Working File (CWF) host sites, standard system maintainers, regional laboratory carriers, claims processing data centers, Data Centers, Enterprise Data Centers (EDCs), and Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC]).

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 - SEC. 912: Requirements for Information Security for Medicare Administrative Contractors" (Section 912 of the MMA) provided for a new type of contractor relationship, the "Medicare Administrative Contractor," and implemented requirements for annual evaluation, testing, and reporting on security programs at both MAC contractors and existing carrier and intermediary business partners (to include their respective data centers). In this manual the terms "business partner" and "contractor" are used interchangeably, and all provisions that apply to business partners also apply to MAC contractors.

This manual addresses the following key business partner security elements:

- An overview of primary roles and responsibilities
- A program management planning table that will assist System Security Officers (SSOs) and other security staff in coordinating system security programs at business partner sites
- Appendix A: The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs), which provides the following:
  - The CSRs
  - An overview of the CISS data collection and reporting process

The CMS IT systems security program and CSRs were developed in accordance with Federal and CMS documents that mandate the handling and processing of Medicare data. These documents include the following:

- CMS *Information Security (IS)* System Security Plans (SSP) *Procedures*, Version *4*.0 *Draft*, *July 10, 2007*

http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage

- Federal Information Security Management Act of 2002 (FISMA), November 27, 2002
  http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

- Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, Electronic Freedom of Information Act of 1996
  http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm

- GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999
  http://www.gao.gov/special.pubs/ai12.19.6.pdf

- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies *and Entities*, *February 2007*
  http://www.irs.gov/pub/irs-pdf/p1075.pdf

- Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (PUBLIC LAW 108–173), DEC. 8, 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors
  http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ173.108.pdf

- Office of Management and Budget (OMB) Circular No. A-127, Financial Management Systems, June 21, 1995
  http://www.whitehouse.gov/omb/circulars/a127/a127.html

- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999
  http://www.whitehouse.gov/omb/circulars/index.html

- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000
  http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

- Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000
  http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

- Presidential Decision Directive/NSC – 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998
  http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

- Public Law 74-271, Social Security Act, as amended, §1816, Use of public agencies or private organizations to facilitate payment to provider of service

http://www.ssa.gov/OP_Home/ssact/title18/1816.htm

- Public Law 74-271, Social Security Act, as amended, §1842, Use of carriers for administration of benefits
  http://www.ssa.gov/OP_Home/ssact/title18/1842.htm

- Public Law 93-579, The Privacy Act of 1974, as amended
  http://www.usdoj.gov/foia/privstat.htm

- Public Law 99-474, Computer Fraud & Abuse Act of 1986
  http://nsi.org/Library/Compsec/cfa.txt

- Public Law 100-235, Computer Security Act of 1987
  http://www.nist.gov/cfo/legislation/Public Law 100-235.pdf

- Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35
  http://www.estrategy.gov/documents/16.pdf

- Public Law 104-106, Clinger-Cohen Act of 1996 (formerly called the Information Technology Management Reform Act)
  http://www.tricare.osd.mil/jmis/download/PublicLaw104_106ClingerCohenActof1996.pdf

- Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA), 1996
  http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAAlawdetail.pdf

Additional documents were used as references in the development of this manual and the CMS CSRs. These documents include the following:

- CMS Information Security *(IS)* Acceptable Risk Safeguards (ARS) Version *3*.0, *September 19, 2007*
  http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage

- CMS Information Security *(IS)* Certification and Accreditation (C&A) *Program Procedures*, Version *3.0.13 Final Draft*, *June 26, 2007*
  http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage

- CMS Information Security Risk Assessment (*IS* RA) *Procedures*, Version *4.0 Draft, July 23, 2007*
  http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage

- CMS Information Security Risk Assessment (RA) and System Security Plan (SSP) Guidance, Version 1.0 September 3, 2004

http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage

- Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability, 5CFR731
  http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html

- United States Code Title 44 Chapter 33—Disposal of Records
  http://www4.law.cornell.edu/uscode/html/uscode44/usc_sup_01_44_10_33.html

- Department of Health and Human Services (HHS), IRM *OCIO* Policies
  http://www.hhs.gov/read/irmpolicy/index.html

- Homeland Security Presidential Directive/HSPD-7*, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003*
  http://www.fas.org/irp/offdocs/nspd/hspd-7.html

- *Homeland Security Presidential Directive/HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004*
  http://www.fas.org/irp/offdocs/nspd/hspd-12.html

- *Homeland Security Presidential Directive/HSPD-20, National Continuity Policy, May 9, 2007*
  http://www.fas.org/irp/offdocs/nspd/nspd-51.htm

- *Federal Information Processing Standards (FIPS) Publication (PUB) 140-3 Draft, Security Requirements for Cryptographic Modules, July 2007*
  http://csrc.nist.gov/publications/PubsFIPS.html

- *FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004*
  http://csrc.nist.gov/publications/PubsFIPS.html

- *FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006*
  http://csrc.nist.gov/publications/PubsFIPS.html

- *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995*
  http://csrc.nist.gov/publications/PubsSPs.html

- *NIST* SP 800-*53 Revision 2, Recommended Security Controls for Federal Information Systems, December 2007*
  http://csrc.nist.gov/publications/PubsSPs.html

- *NIST SP 800-53A Final Public Draft, Guide for Assessing the Security Controls in Federal Information Systems, December 2007*
  http://csrc.nist.gov/publications/PubsSPs.html

- *NIST SP 800-61, Computer Security Incident Handling Guide, September 28, 2007*
  http://csrc.nist.gov/publications/PubsSPs.html

- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004
  http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html.

- CMS Policy for the Information Security Program, CMS-CIO-POL-SEC02-*02 Draft*, *August 24, 2007*
  http://www.cms.hhs.gov/InformationSecurity/13_Policies.asp#TopOfPage

1.1 Additional Requirements for MAC Contractors

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

MAC contractors are responsible for fulfilling all existing business partner requirements. Additional requirements are specified in Section 912 of the Medicare Modernization Act (MMA). These additional requirements include the following:

- The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 days of receipt of the final audit or evaluation report, unless otherwise authorized by CMS.

  The contractor shall comply with the CMS Certification and Accreditation (C&A) methodology, policies, standards, procedures, and guidelines for contractor facilities and systems. The CMS *IS* C&A *Program Procedures* can be found on the CMS *Web* site at:
  http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage

- The contractor shall conduct or undergo an independent evaluation and test of its system security program in accordance with Section 912 of the MMA. The first test shall be completed before the contractor commences claims payment under the contract.

- The contractor shall support CMS validation and accreditation of contractor systems and facilities in accordance with the CMS *IS* C&A *Program Procedures*.

- The contractor shall provide annual certification, in accordance with the CMS *IS* C&A *Program Procedures*, that they have examined the management, operational, and technical controls for its systems supporting the MAC function, and consider these controls adequate to meet CMS security standards and requirements.

- The contractor shall appoint a Chief Information Officer (CIO) to oversee its compliance with the CMS security requirements. The contractor's Systems Security Officer (SSO) shall be a full-time position dedicated to assisting the CIO in fulfilling these requirements.

2 IT Systems Security Roles and Responsibilities

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

2.1 CMS Project Officer (PO)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS POs (generally located in Central Office business components) oversee the other business partners and also have Federal Acquisition Regulation (FAR) responsibilities at data centers. The PO has the following responsibilities:

- CMS point of contact for business partner IT systems security problems

- Central point for the reception of IT SSPs and reports including security incident reports

- Provider of technical assistance necessary to respond to CMS security policies and procedures

2.2 The (Principal) Systems Security Officer (SSO)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners *shall* designate an SSO qualified to manage the Medicare system security program and ensure the implementation of necessary safeguards. The SSO *shall* be organizationally independent of IT operations. The SSO can be within the CIO organizational domain but cannot have responsibility for operation, maintenance, or development.

The SSO position for each contractor should be full-time and fully qualified—preferably credentialed in systems security (e.g., Certified Information Systems Security Professional [CISSP]). Having an individual with appropriate education and experience to execute security administration duties will help reinforce that security must be a cultural norm that guides daily activities, and not a set of compliance directives. A

qualified SSO who is available to direct security operations full-time provides the foundation for the security culture and awareness of the organization.

A sound entity-wide security program is the cornerstone of effective security control implementation and maintenance. Security controls cannot be effective without a robust entity-wide security program that is fully sponsored and practiced by management, and staffed by individuals with proper training and knowledge. Contractors should also encourage their systems security personnel to pursue security accreditation using available funding.

A business partner may have additional SSOs at various organizational levels, but all security actions *shall* be coordinated through the principal SSO for Medicare records and operations. The SSO ensures compliance with CMS CSRs by:

- Facilitating the Medicare IT system security program and ensuring that necessary safeguards are in place and working
- Coordinating system security activities throughout the organization
- Ensuring that IT system security requirements are considered during budget development and execution
- Reviewing compliance of all components with the CMS CSRs and reporting vulnerabilities to management
- Establishing an incident response capability, investigating system security breaches, and reporting significant problems (see section 3.6) to business partner management.
- Ensuring that technical and operational security controls are incorporated into new IT systems by participating in all business planning groups and reviewing all new systems/installations and major changes
- Ensuring that IT systems security requirements are included in Requests for Proposal (RFP) and subcontracts involving the handling, processing, and analysis of Medicare data
- Maintaining systems security documentation in the System Security Profile for review by CMS and external auditors
- Cooperating in all official external evaluations of the business partner's system security program
- Facilitating the completion of the Risk Assessment (see section 3.2)

- Ensuring that an operational IT Systems Contingency Plan is in place and tested (see section 3.4)

- Documenting and updating the monthly Plan of Action and Milestones (POA&M) (see section 3.5.2). Updates may occur whenever a POA&M projected completion date passes, and following the issuance of new requirements, risk assessments, internal audits, and external evaluations. The schedule and updates are highly sensitive and should have limited distribution.

- Keeping all elements of the business partner's System Security Profile secure (see section 3.7)

- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix B)

The Principal SSO should earn a minimum of 40 hours in continuing professional education credits each year from a recognized national information systems security organization. The educational sessions at the CMS Security Best Practices Conference can be used toward fulfilling CMS business partners' continuing professional education credits. The qualifying sessions and associated credit hours will be noted on the CMS Security Best Practices Conference agenda.

2.3 *Business* Owners

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partner *Business* Owners are responsible for:

- Determining and documenting the information and information system security levels of the resources for which they are responsible

- Identifying appropriate security level categorizations for their information and information systems

2.4 System Maintainers/Developers

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partner System Maintainers/Developers have the responsibility to implement the security requirements throughout the System Development Life Cycle (SDLC).

2.5 Personnel Security/Suitability

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All business partner and contractor employees requiring access to CMS sensitive information *shall* meet minimum personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title, and favorable results from a background check. The background check for

prospective and existing employees (if not previously completed) should include, at a minimum: contacting references provided by the employee and contacting the local law enforcement agency or agencies.

3 IT Systems Security Program Management

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners *shall* have policies and procedures, and implement controls or plans that fulfill the CMS CSRs (see *applicable* Attachment).

Policies are formal, up-to-date, documented rules stated as "shall" or "will" statements that exist and are readily available to employees. They establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness. Policies are written to cover all major facilities and operations corporate-wide or for a specific asset (e.g., Medicare claims processing), and they are approved by key affected parties. Policies delineate the IT security management structure, clearly assign IT security responsibilities, and lay the foundation necessary to reliably measure progress and compliance. Policies also identify specific penalties and disciplinary actions to be used in the event that the policy is not followed.

Procedures are formal, up-to-date, documented instructions that are provided to implement the security controls identified by the defined policies. They clarify where the action is to be performed, how the action is to be performed, when the action is to be performed, who is to perform the action, and on what the action is to be performed. Procedures clearly define IT security responsibilities and expected behaviors for: asset owners and users, information resources management and data processing personnel, management, and IT security administrators. Procedures also indicate appropriate individuals to be contacted for further information, guidance, and compliance. Finally, procedures document the implementation of, and the rigor with which, the control is applied.

Controls are measures implemented to protect the confidentiality, integrity, and availability of sensitive information. IT security procedures and controls shall be implemented in a consistent manner everywhere that the procedure applies. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. In addition, initial testing shall be performed to ensure that controls are operating as intended.

Meeting requirements does not validate the quality of a program. Managers with oversight responsibility *shall* understand the processes and methodology behind the requirements. Table 3.1 identifies key requirements and provides high-level descriptions for them. As appropriate, Table 3.1 refers to other parts of this document that provide details on ways to accomplish each requirement. Business partners *shall* perform a *FISMA Evaluation*[1] using the CISS. The weaknesses, action plans, and POA&Ms *shall*

be recorded in the CISS (See Appendix A). To perform the *FISMA Evaluation*, business partners *shall* conduct a systematic review of the CSRs using the CISS. The CISS provides a *FISMA Evaluation* form that includes guidance and audit protocols to assist in the review of the requirements.

The CMS CSRs include key security-related tasks. Table 3.1 indicates how often these tasks need to be performed, the disposition of output or documentation, comments, and a space to indicate completion or a "do by" date. The number accompanying each entry in the requirement column indicates the section in this document that deals with the particular requirement. Use this table as a checklist to ensure that all required IT systems security tasks are completed on schedule. Consult the referenced sections for clarifying details.

Table 3.1. Reporting Requirements Planning Table

Requirement	Frequency	Send To	Comments	Complete (check when complete)
Appendix A, *FISMA Evaluation* using the CISS	*One third of the controls shall be tested e*ach Federal FY *so all controls are tested during a three (3) year period.*	▪ PO with a copy to CMS CO ▪ System Security Profile	See Appendix A for an overview of the *FISMA Evaluation*. *FISMA Evaluation* results recorded using the CISS are to be discussed in the Certification Package.	
3.1 *Information Security (IS)* System Security Plans *(SSP)*	The *IS* SSP for each GSS & MA *shall* be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change[2].	▪ SSO ▪ CMS CO ▪ System Security Profile	*IS* SSPs are to be reviewed, updated, and certified by management and indicated as such in both the Certification Package/ *S*tatement of *C*ertification and the System Security Profile[3].	
3.2 *Information Security* Risk Assessment *(IS RA)* (Report)	The *IS RA* for each GSS and MA *shall* be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change.[1]	▪ CMS CO ▪ System Security Profile	*IS* R*A*s are to be reviewed, updated, and certified by management and indicated as such in both the Certification Package/ *S*tatement of *C*ertification and the System Security Profile. The *IS RA* Report *is* submitted with the *IS* SSP[4].	
3.3 Certification	Each Federal FY	▪ PO with a copy to CMS CO ▪ System Security Profile	Fiscal intermediaries and carriers should include a statement of certification as part of their CPIC package. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-6) information on certification requirements including where, when, and to whom these certifications *shall* be submitted. All other contractors should submit a statement of security certification to their CMS POs.	

[2] NIST defines "significant change" as "any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."

[3] More information about system security planning can be found in the CMS SSP Methodology.

[4] More information about Risk Assessment Reports can be found in the CMS Information Security Risk Assessment (RA) Methodology.

Requirement	Frequency	Send To	Comments	Complete (check when complete)
3.4 IT Systems Contingency Plan *(CP)*	CPs *shall* be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change.[1] *CP*s *shall* be tested annually.	▪ SSO ▪ CMS CO ▪ System Security Profile	Management and the SSO *shall* approve the *CP*. The IT Systems *CP* is to be developed (in accordance with Appendix B), reviewed, updated, and certified by management—and indicated as such in both the Certification Package/*S*tatement of *C*ertification and the System Security Profile[5].	
3.5 Compliance	Each Federal FY	▪ SSO ▪ PO ▪ CMS CO ▪ System Security Profile	**POA&M**: POA&Ms address *Findings* of annual system security assessments including the annual *FISMA Evaluation*, and, as applicable: SAS 70 audits, CFO controls audits, the Section 912 evaluation, and data center tests and reviews.	
3.6 Incident Reporting and Response	As necessary	▪ PO ▪ System Security Profile	HIPAA also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file with the Principal SSO		

LEGEND:

CFO	Chief Financial Officer
CISS	CMS Integrated Security Suite
CO	Central Office (CMS)
CP	*Contingency Plan*
CPIC	Certification Package for Internal Controls
FY	Fiscal Year
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
MA	Major Application
PO	Project Officer (CMS)
POA&M	Plan of Action and Milestones
RA	*Risk Assessment*
SAS	Statement on Auditing Standard
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer
SSP	System Security Plan

NOTE: Documents listed in table 3.1 may be stored as paper documents, electronic documents, or a combination thereof.

When submitting documentation to the CMS Central Office, registered mail or its equivalent (signed receipt required) should be used. For supporting documentation (such as Risk Assessments, Contingency Plans, System Security Plans, etc.), only digital soft copies in the approved CMS format are required. Paper copies are only required for

[5] More information about contingency planning can be found in An Introduction to Computer Security: The NIST Handbook. SP 800-12, and the Contingency Planning Guide for Information Technology Systems: NIST Special Pub 800-34.

certification signature pages, certifying the completion of required periodic document development, review, updates, and certification. Contact addresses are as follows:

Program Safeguard Contractors *(PSCs)*

- CMS Central Office
  Office of Financial Management
  Program Integrity Group
  Mail Stop C3-02-16
  7500 Security Blvd.
  Baltimore, MD 21244-1850

Common Working File *(CWF) and* Shared System Maintainers

- CMS Central Office
  Office of Information Services
  Business Application and Management Group
  Mail Stop N3-13-27
  7500 Security Blvd.
  Baltimore, MD 21244-1850

Fiscal Intermediaries /Carriers/ Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC])

- CMS Central Office
  Centers for Medicare Management
  Medicare Contractor Management Group
  Mail Stop S1-14-17
  7500 Security Blvd.
  Baltimore, MD 21244-1850

Data Centers *and* Enterprise Data Centers (EDC)

- CMS Central Office
  Office of Information Services
  Enterprise Data Center Group
  Mail Stop N1-19-18
  7500 Security Blvd.
  Baltimore, MD 21244-1850

3.1 System Security Plan (SSP)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The objective of an information security program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process or store Medicare-related data have some level of sensitivity and require protection. The protection of a system *shall* be documented in an *IS* SSP. The completion of an SSP is a requirement of OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law

100-235, the Computer Security Act of 1987. All Medicare claims-related applications and systems categorized as either a Major Application (MA) or General Support System (GSS) *shall* be covered by SSPs.

The purpose of an SSP is to provide an overview of the security requirements of a system and describe the controls that are implemented to meet those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate and cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager (i.e., SSO).

All business partners are required to maintain current SSPs for their Medicare claims-related GSSs and MAs in their System Security Profiles. The SSP documents the current level of security within the system or application; that is, actual implemented controls, not planned controls. In addition, the SSP serves as the primary documentation reference for testing and evaluation, whether by CMS, the General Accounting Office (GAO), or other oversight bodies. The SSP is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. Therefore, these security plans should be distributed only on a need-to-know basis.

The SSPs *shall* be available to the SSO and business partner certifying official (normally the VP for Medicare Operations), and authorized external auditors as required. The SSO and *Business* Owner are responsible for reviewing the SSP on an annual basis to ensure that it is up-to-date. The objective of these annual reviews is to verify that the controls selected or installed remain adequate to provide a level of protection to reach an acceptable level of risk to operate the system.

All business partner Medicare claims-related SSPs *shall* be developed in accordance with the most current version of the CMS *Information Security (IS)* System Security Plan (SSP) *Procedures* and the CMS Information Security *Risk Assessment (*RA*)* and *System Security Plan (*SSP*)* Guidance, both of which are available on the CMS Web site at: *http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage*. Business partners *shall* also use the most current version of the Microsoft® Word© SSP template, available at the same Web site.

SSPs *shall* be re-certified within 365 days from the last date certified. The SSP *shall* also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update to the SSP needs to occur. The SSP *shall* be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review and the updated SSP, if applicable, *shall* be placed in the Medicare contractor's System Security Profile, and a copy *shall* be provided to the CMS Central Office.

Contractors updating their current SSP(s) or developing new SSP(s) *shall* include Medicare claims processing front-end, back-end, and/or other claims processing related systems using the most current version of the CMS *Information Security (IS)* System Security Plan *(SSP) Guidance*. The CMS *SSP guidance* and template *are available* on the CMS *Web site* at:
http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage.

Front-end systems are those systems Medicare contractors develop and maintain for use in their operations areas and data centers to enter claims and claims-related data into the standard/shared claims processing system. These front-end systems include, but are not limited to: electronic data interchange, imaging systems, optical character recognition, manual claims entry, claims control, provider, beneficiary, other payer databases, and other pre-claims processing business functions. Back-end systems are those systems that Medicare contractors develop and maintain for use in their operations areas and data centers to output claims processing information (i.e., checks, Medicare summary notices, letters, etc). These back-end systems include, but are not limited to: print mail, 1099, post-payment medical reviews, customer service, appeals, overpayment written/phone inquiries and separate claims reconciliation systems.

A newly developed or updated SSP *shall* be sent in electronic form to the CMS Central Office on CD-ROM. This CD-ROM must be received by CMS ten (10) working days after the SSP(s) has been developed, updated, or re-certified. The original signed, dated CMS SSP certification form *shall* be submitted in hard copy along with the electronic CD-ROM copy. This information should not be submitted to the CMS Central Office via email—registered mail or its equivalent (signed receipt required) should be used.

In summary, the SSP *shall* be updated and re-certified annually unless there are changes as discussed above that would necessitate a more frequent update. Should SSP technical assistance be required, direct all questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/Northrop Grumman Help Desk at 703-272-5725.

3.2 Risk Assessment

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners are required to perform an annual risk assessment in accordance with the CMS Information Security *Risk Assessment (IS* RA*) Procedures* and the CMS Information Security *Risk Assessment (*RA*)* and *System Security Plan (*SSP*)* Guidance. These documents are available at *the CMS Web site*:
http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage.

The CMS *IS* RA *Procedures* presents a systematic approach for the RA process of Medicare information computer systems within the CMS and business partner environments. The *procedures* describe the steps required to produce an *IS* RA Report for systems and applications that require an SSP. This *procedure* and its resultant report replace the former Triennial RA requirement and report.

All system and information owners *shall* develop, implement, and maintain risk management programs to ensure that appropriate safeguards are taken to protect all CMS resources. A risk-based approach shall be used to determine adequate security and shall include a consideration of the major factors in management such as the value of the system or application, all threats, all vulnerabilities, and the effectiveness of current or proposed safeguards. The CMS *IS* RA *Procedures shall* be used to prepare an annual *IS* RA Report.

All RAs *shall* be re-certified within 365 days from the last date certified. Medicare contractors *shall* review their RA(s) prior to re-certification to determine if an update is needed. An RA *shall* be performed if a significant change to any information system has occurred. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review and/or the updated RA *shall* be placed in the Medicare contractor's System Security Profile. The updated RA(s) *shall* also be mailed to the CMS Central Office. The RA used to support a SSP(s) cannot be dated more than 12 months earlier than the SSP certification date.

Contractors that must update their current RA(s) *shall* use the most current version of the CMS Information Security *Risk Assessment (IS* RA*) Procedures*. The CMS *procedures* and template *are available* on the CMS *W*eb site at: *http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage*.

A newly developed or updated RA that is submitted with the SSP *shall* be sent to the CMS Central Office on CD-ROM. This CD-ROM must be received by CMS ten (10) working days after they have been developed or updated. This information should not be submitted to the CMS Central Office via email—registered mail or its equivalent (signed receipt required) should be used.

In summary, the RA *shall* be updated annually unless there are changes to either as discussed above that would necessitate a more frequent update. Should RA technical assistance be required, direct all questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/Northrop Grumman Help Desk at 703-272-5725.

Business partners should refer to the CMS Information Security *(IS)* Acceptable Risk Safeguards (ARS) document to aid in the preparation of a risk assessment. This document *is available on the CMS Web site* at: *http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage*.

3.3 Certification

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All Medicare business partners are required to certify their system security compliance. Certification is the formal process by which a contract official verifies, initially and then by annual reassessment, that a system's security features meet CMS CSRs. Business partners *shall* self-certify that their organization(s) successfully completed a security *FISMA Evaluation* of their Medicare IT systems and associated software in accordance with the terms of their Medicare Agreement/Contract.

Each contractor is required to self-certify to CMS its IT systems security compliance within each Federal fiscal year. This security certification *shall* be included in the Certification Package for Internal Controls (CPIC) or, for contracts not required to submit CPIC certifications, send the security certification to their appropriate CMS POs. CMS will continue to require annual, formal re-certification within each fiscal year no later than September 30, including validation at all levels of security as described in this manual.

Systems security certification *shall* be fully documented and maintained in official records. The security certification validates that the following items have been developed (i.e., updated and/or reviewed, as required) and are available for review in the System Security Profile:

- Certification
- *FISMA Evaluation* (see *section 3.5.2 and* Appendix A)
- System Security Plan for each GSS and MA (see section 3.1)
- Risk Assessment (see section 3.2)
- IT Systems Contingency Plan (see section 3.4 and Appendix B)
- Plan of Action and Milestones (see section 3.5.*3*)

3.4 Information Technology (IT) Systems Contingency Plan

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All business partners are required to develop and document an IT Systems Contingency Plan that describes the arrangements that have been made and the steps that *shall* be taken to continue IT and system operations in the event of a natural or human-caused disaster. Medicare IT Systems Contingency Plans *shall* be included in management planning and *shall* be:

- Reviewed whenever new systems are planned or new safeguards contemplated

- Reviewed annually to ensure that they remain feasible

- Tested annually. If backup facility testing is done *by Medicare contract type (i.e., when multiple contract types are involved [e.g., Data Center, Part A/B, DMERC])*, each individual Medicare *contract type shall be tested* every year.

Appendix B to this manual provides information on Medicare IT Systems Contingency Plans and testing methods. See Item 3.4 in Table 3.1, section 3.0, for other references.

Each Medicare contractor *shall* review its IT Systems Contingency Plan 365 days from the date it was last reviewed or updated to determine if changes to the contingency plan are needed. A contingency plan should be updated if a significant change has occurred. The system contingency plan *shall* also be tested 365 days from the last test performed. Updated plans and test reports (results) should be placed in the contractor's System Security Profile. Business partner management and the SSO *shall* approve newly developed or updated IT Systems Contingency Plans. Information on Medicare IT systems contingency planning can be found in Appendix B.

A newly developed or updated Medicare IT System Contingency Plan *shall* be submitted to CMS within 10 (ten) working days after the business partner's management and SSO have approved it. A copy of the IT System Contingency Plan *shall* be submitted via CD-ROM to the CMS Central Office along with a hard copy of the statement of certification. This information should not be submitted via email. Registered mail or its equivalent should be used.

3.5.2 Annual FISMA Evaluation (FE)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A critical factor for maintaining on-going compliance with FISMA and the Federal Managers' Financial Integrity Act of 1982 (FMFIA) is for Business Owners in coordination with developers / maintainers, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing) and person-hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of applicable POA&Ms for vulnerabilities noted during the annual testing.

The purpose of annual FE testing (i.e., validation) is to examine and analyze implemented security safeguards in order to provide evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. The annual FE is intended to validate the security controls to determine the extent to which the controls are:

- *implemented correctly,*
- *operating as intended, and*
- *producing the desired outcome with respect to meeting the security requirements for the system.*

To fulfill the annual FE validation obligation, the FE shall be conducted by an independent agent or team. This can be any internal or external agent or team that is capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain of command associated with the information system or to the determination of security control effectiveness.

The annual FE testing requirement has been interpreted by OMB as being within 365 calendar days of the prior test. Over a three (3) year period, all controls applicable to a system or application shall be tested. This means a subset (no less than one-third [$^{1}/_{3}$]) of the security controls shall be tested each year so that all controls are tested during a three (3) year period.

While CMS does not mandate which subset of controls should be tested each year or require a specific number of controls to be tested each year, CMS (and OMB) does require that all controls be tested within a three (3) year period. Business Owners, in coordination with the developers / maintainers of CMS applications and systems, are responsible for meeting this requirement.

All management directed testing may be used to meet the requirement for the annual FE testing. Management directed testing includes: independent Security Test and Evaluations (ST&E), testing performed pursuant to CMS compliance with OMB Circular A-123, evaluations and tests conducted under authority of Section 912 of the MMA, Statement on Auditing Standards (SAS) No. 70 internal control reviews, and test results from local test teams organized for purposes of meeting this requirement.

Annual security controls testing, including FE testing, should be used to satisfy the requirements for the ST&E which is an integral component of the CMS Certification and Accreditation (C&A) Program. In order to be considered as part of a system's or application's ST&E, the annual security control testing shall meet the standards for independence.

3.5.*3* Plan of Action and Milestones (POA&Ms)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners are required to submit a monthly POA&M package which is due by the 1st of each month. The POA&M package consists of a CISS-generated POA&M data file and, if required by CMS, any additional supporting documentation.

3.5.*3*.1 Background

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The FISMA requires that Federal agencies provide annual reporting of the state of security programs for all IT systems associated with the agency. Additionally, periodic POA&Ms reporting the status of known security weaknesses for all Federal agency systems *shall* also be submitted to the OMB. This reporting requirement applies to a broader scope of security weaknesses, as it is not limited to weaknesses identified by specific audits and reviews (such as those covered under FMFIA). In the case of FISMA, any security weakness identified for covered systems *shall* be reported and included in a periodic POA&M report.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for both MAC contractors and existing carrier and intermediary business partners (to include their respective data centers). These Section 912 evaluations and reports necessitate an annual on-site review of business partner security programs to ensure that they meet the information security requirements imposed by FISMA. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified deficiencies be addressed in a report to be submitted shortly after the evaluation results are finalized, as well as periodically thereafter to track updated progress towards completion of the identified action plans.

The CISS enables contractors to satisfy reporting requirements for EDP security-related findings. Security-related finding (and approved action plan) data is entered into the CISS following all audits/reviews, from which the CISS generates a single monthly submission data file that summarizes the current state of security for the business partner. This data file is submitted to CMS as part of the monthly POA&M package.

3.5.3.2 POA&M Package Components/Submission Format

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

In addition to the initial POA&M reporting that follows each audit/review, summary POA&Ms shall be submitted on the 1st of each month via the CISS. The CISS shall be populated with EDP security-related findings from the Chief Financial Officer's Electronic Data Processing (CFO EDP) Audit, the Section 912 evaluation, *Data Center ST&E*, the SAS 70 review, the Certification Package of Internal Controls (CPIC), and any other EDP security-related findings that result from an audit or review, whether internal or external. Corrective actions are to be established in the CISS to address all resulting weaknesses entered therein, and those corrective actions *shall* be reflected in the CISS POA&M (both in the data file and reports).

To ensure consistency, all Medicare contractors *shall* enter into the CISS the Section 912 evaluation, Data Center ST&E, and/or CFO EDP Audit POA&Ms that have already been accepted and approved by CMS for its EDP findings, as the standard for all future submitted POA&Ms. Findings from other audits, reviews and evaluations (e.g., SAS 70,

CPIC, internal audits, etc.) that address the same security finding problem should use the same solution (action plan) if it will adequately resolve the identified weakness.

Initial Report. Within 45 days (or as otherwise directed by CMS) of the final results for every internal/external audit/review, an initial, manually generated, CMS POA&M Weakness Tracking Form is due to CMS that describes the findings of the audit/review and initial corrective actions planned for implementation. Upon acceptance from CMS, this information will be entered into the CISS by the Medicare contractor for monthly tracking purposes.

NOTE: Medicare contractors are encouraged to use the draft reports (when available) to prepare their corrective actions for identified findings.

Monthly POA&M Package. On a monthly basis, business partners shall provide updates on progress towards completion of remediation efforts for weaknesses identified from all known sources. The monthly POA&M package shall include a CD-ROM that contains the CISS-generated data file at its root level (refer to the POA&M submission instructions in the CISS User Guide). The naming convention for this file is XXX_POAM(XX-01-200X).mdb where XXX is the acronym for the contractor*/entity*, and the date is the due date of the report.

Medicare contractors *shall* submit the monthly POA&M package to the CMS Central Office (for Title XVIII and MAC contracts) or PO (for FAR contracts). This information should not be submitted via email. Registered mail or its equivalent should be used. A copy *shall* also be placed in the System Security Profile.

3.5.*4* Annual/Yearly Compliance Condition

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Many security documents, such as Risk Assessments, SSPs, Contingency Plans, as well as many CMS CSR control techniques (see Appendix A) require annual or yearly performance (e.g., test, submission, recertification, review, update). When such a requirement is to be performed annually or yearly, it is to be performed no later than the one year anniversary date of its previous performance (i.e., within 365 days [366 days in leap years]). The only exceptions to this annual/yearly compliance condition are deliverables whose annual due date are set and distributed by CMS, such as the annual *FISMA Evaluation* submission.

If the *business partner* wishes to change the timing cycle of an annual or yearly requirement compliance date, the *business partner shall* shorten the timing cycle and not lengthen the annual/yearly timing cycle to attain the new performance date. For example, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the *business partner* desired to change the review date to 5/31/07, they would be required to review the SSP no later than 7/31/06 and again no later than 5/31/07, and no later than 5/31/xx thereafter. However, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the *business partner* desired to change the review date to 9/30/06, they

would be required to review the SSP no later than 7/31/06 and again no later than 9/30/06. The next review cycle would then be no later than 9/30/07 and 9/30/XX thereafter.

3.6 Incident Reporting and Response

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

An incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction.* The business partner *shall* use its security policy and procedures to determine whether the security incident is reportable (as defined below). Upon receiving notification of an IT systems security incident or a suspected incident, the SSO *shall* immediately perform an analysis to determine if an incident actually occurred. The incident could result in adversely impacting the processing of Medicare data or the privacy of Medicare data. Reportable incidents include:

- **Unauthorized Disclosure:** *I*nformation disclosure with risk to privacy information or public relations impact
- **Denial of Service:** *A*n attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- **Malicious Code:** *A* virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- **Unauthorized Access:** *A* breach in which person gains logical or physical access to network, system application, data or other resource without permission
- **Inappropriate Usage:** *A* violation of acceptable computing use policies
- **Multiple Components:** *A* single incident that encompasses two or more incidents

3.6.1 Computer Security Incident Response

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All suspected information security incidents or events shall be reported to the CMS IT Service Desk (or equivalent business partner function) as soon as an incident comes to the attention of a CMS information or information system user. All confirmed security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS Information Security Incident Handling and Breach Analysis/Notification Procedure. This document is available on the CMS Web site at http://www.cms.hhs.gov/InformationSecurity/15_Procedures.asp#TopOfPage. The CMS

IT Service Desk can be contacted by telephone at 410-786-2580 or by e-mail at: cms it service desk~cms.hhs.gov.

All CMS contractors and business partners shall utilize the following incident categories, Table 3.2, and reporting time criteria, Table 3.3, when reporting incidents to CMS.

Table 3.2. Incident Categories

Category	*Name*	*Description*
CAT 0	*Exercise /Network Defense Testing*	*Used during State, Federal, national, international exercises, and approved activity testing of internal/external network defenses or responses.*
CAT 1	*Unauthorized Access**	*A person gains logical or physical access without permission to a network, system, application, data, or other resource.*
CAT 2	*Denial of Service**	*An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.*
CAT 3	*Malicious Code**	*A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.*
CAT 4	*Inappropriate Usage**	*A person violates acceptable computing use policies.*
CAT 5	*Probes and Reconnaissance Scams*	*This category includes any activity that seeks to access or identify a Federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.*
CAT 6	*Investigation*	*Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.*
PII	*Personally Identifiable Information (PII) Exposure*	*Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual.*

**Source: NIST SP 800-61*

Table 3.3. Incident Reporting Timeframe Criteria

Category	*Reporting Timeframe*
CAT 0	*Not applicable; this category is for CMS' internal use during exercises.*
CAT 1	*Within one (1) hour of discovery /detection.*
CAT 2	*Within two (2) hours of discovery /detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.*
CAT 3	*Daily; within one (1) hour of discovery /detection if widespread across agency.*
CAT 4	*Weekly.*
CAT 5	*Not applicable; this category is for classified systems.*
CAT 6	*Not applicable; this category is for CMS' use to categorize a potential incident that is currently being investigated.*
PII	*Within one (1) hour of discovery /detection.*

When reporting confirmed security incidents, business partners should report the date and time when events occurred or were discovered; names of systems, programs, or networks effected by the incident; and impact analysis. Release of information during incident handling *shall* be on an as-needed and need-to-know basis. When other entities should be notified of incidents at external business partner sites, CMS will coordinate with legal and public affairs contacts at the effected entities. If a violation of the law is suspected, CMS will notify the Office of the Inspector General's (OIG) Computer Crime Unit and submit a report to the FedCIRC of the incident with a copy to the CMS Senior Information Systems Security Office.

As part of the risk management process, the business partner should determine the extent of the incident's impact and the potential for new or enhanced controls required to mitigate newly identified threats. These new security controls (and associated threats and impacts) should provide additional input into the business partner's risk assessment. Business partners should refer to The CMS *Information* Security Incident Handling *and Breach Analysis/Notification* Procedure for further guidance.

3.7 System Security Profile

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Consolidate security documentation (paper documents, electronic documents, or a combination) into a System Security Profile that includes the following items:

- Completed *FISMA Evaluation*
- System Security Plan (for each GSS and MA)
- Risk Assessments
- Certifications

- IT Systems Contingency Plans
- POA&Ms for each compliance security review
- POA&Ms for other security review undertaken by HHS OIG, CMS, IRS, GAO, consultants, subcontractors, and business partner security staff
- Incident reporting and responses
- Systems security policies and procedures

The System Security Profile shall be kept in a secure location, kept up-to-date, and pointers to other relevant documents maintained. A backup copy of the System Security Profile shall be kept at a secure off-site storage location, preferably at the site where back-up tapes and/or back-up facilities are located. The back-up copy of the profile shall also be kept up-to-date, particularly the contingency plan documents.

3.10.1 Security Configuration Management

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires NIST to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal *g*overnment.

CMS security configuration management guidance, including DHHS requirements and links to NIST, NSA, and DISA configuration guides are provided in Appendix F.

CMS does not require the verbatim use of these guidance documents and tools for the configuration of Medicare systems. However, CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity. CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

NOTE: DMEMACs, ABMACs, and EDCs are required to start with these Security Technical Implementation Guide (STIG) baseline configurations and then document any exceptions based on environment specific implementation.

3.10.2 National Institute of Standards and Technology (NIST)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS, as a government agency, highly encourages business partners to review and incorporate the NIST concepts into their Medicare security program. Under the Computer

Security Act of 1987 (P.L. 100-235), NIST develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on IT security issues. The publications are issued as Federal Information Processing Standards Publications (FIPS), Special Publications (SP), NIST Interagency Reports (NISTIRs), and IT Laboratory (ITL) Bulletins.

Special Publications in the 800 series (SP 800-XX) present documents of general interest to the computer security community. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (P.L. 104-106) and the Computer Security Act of 1987 (P.L. 100-235). With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, references to the "waiver process" contained in many of the FIPS are no longer operative. Note, however, that not all FIPS are mandatory; consult the applicability section of each FIPS for details.

CMS does not normally require the verbatim use of NIST S*P*s for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are *specified* in the CMS BPSSM and the CMS CSRs. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop security standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

Table 3.*4* contains a listing of NIST publications relevant to common systems or technology utilized within the Medicare business partner community. Table 3.*4* is not meant to be all-inclusive and may contain some references that are not applicable to a particular Medicare business partner application. The most current NIST publications *are available* at*:* http://csrc.nist.gov/publications/index.html.

Table 3.*4*. NIST Publications

Publication Number	Title
SP 800-113 (Draft)	*Guide to SSL VPNs*
SP 800-111 (Draft)	*Guide to Storage Encryption Technologies for End User Devices*
SP 800-110 (Draft)	*Information System Security Reference Data Model*
SP 800-103 (Draft)	An Ontology of Identity Credentials, Part I: Background and Formulation
SP 800-101	Guidelines on Cell Phone Forensics
SP 800-100	Information Security Handbook: A Guide for Managers
SP 800-98	*Guidelines* for Securing Radio Frequency Identification (RFID) Systems

Publication Number	Title
SP 800-97	*Establishing Wireless Robust Security Networks: A Guide to* IEEE 802.11i
SP 800-96	Personal Identity Verification (PIV) Card / Reader Interoperability Guidelines
SP 800-95	Guide to Secure Web Services
SP 800-94	Guide to Intrusion Detection and Prevention Systems *(IDPS)*
SP 800-92	Guide to Computer Security Log Management
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-88	Guidelines for Media Sanitization
SP 800-86	Guide to *Integrating* Forensic Techniques *in*to Incident Response
SP 800-85A	PIV Card Application *and Middleware Interface* Test Guidelines
SP 800-85B	PIV Data Model Conformance Test Guidelines
SP 800-84	Guide to *Test, Training, and Exercise Programs for IT Plans and Capabilities*
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-82 *(Draft)*	Guide to Industrial Control Systems *(ICS)* Security
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-80 (Draft)	Guide for Developing Performance Metrics for Information Security
SP 800-79	Guidelines for the C&A of PIV Card Issuing Organizations
SP 800-78 *Rev. 1*	Cryptographic Standards and Key Sizes for PIV
SP 800-77	Guide to IPsec VPNs
SP 800-76 *Rev. 1*	Biometric Data Specification for PIV
SP 800-73 Rev. *2*	*Interfaces for PIV (4 parts): 1- Card Application Namespace, Data Model & Representation 2- Card Appl. Card Command Interface 3- Client Appl. Programming Interface 4- Transitional Interfaces & Data Model*
SP 800-72	Guidelines on PDA Forensics
SP 800-70	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process

Publication Number	Title
SP 800-64 Rev. 1	Security Considerations in the Information System Development Life Cycle
SP 800-63 *Ver*. 1.0.2	Electronic Authentication Guideline: Recommendations of the NIST
SP 800-61 *Rev. 1*	Computer Security Incident Handling Guide
SP 800-60 Vols. 1&2	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-59	Guideline for Identifying an Information System as a National Security System
SP 800-58	Security Considerations for Voice Over IP (VoIP) Systems
SP 800-57	Recommendation *for* Key Management
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-55 *Rev. 1 (Draft)*	*Performance Measurement* Guide for *Information Security*
SP 800-54	*Border Gateway Protocol Security*
SP 800-53A *(Final Draft)*	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-53 Rev. *2*	Recommended Security Controls for Federal Information Systems
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-50	Building an IT Security Awareness and Training Program
SP 800-49	Federal S/MIME V3 Client Profile
SP 800-48 *Rev. 1 (Draft)*	Wireless Network Security *for IEEE* 802.11*a/b/g and* Bluetooth
SP 800-47	Security Guide for Interconnecting IT Systems
SP 800-46, *Ver. 2 (Draft)*	*User's Guide to Securing External Devices for Telework and Remote Access*
SP 800-45 *Ver. 2*	Guidelines on Electronic Mail Security
SP 800-44 *Ver. 2*	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Windows 2000 Professional
SP 800-42	Guideline on Network Security Testing
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-40 Ver. 2	Creating a Patch and Vulnerability Management Program
SP 800-37	Guide for the Security C&A of Federal Information Systems
SP 800-36	Guide to Selecting *IT* Security Products
SP 800-35	Guide to IT Security Services
SP 800-34	Contingency Planning Guide for IT Systems
SP 800-33	Underlying Technical Models for IT Security
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure

Publication Number	Title
SP 800-30	Risk Management Guide for IT Systems
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
SP 800-28 *Ver. 2 (Draft)*	Guidelines on Active Content and Mobile Code
SP 800-27 Rev. A	Engineering Principles for IT Security (A Baseline for Achieving Security)
SP 800-26 Rev. 1	Guide for Information Security Program Assessments and System Reporting Form *-- WITHDRAWN*
SP 800-25	Federal Agency Use of *Public Key Technology* for Digital Signatures and Authentication
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-21 *Rev.* 1	*2nd Edition,* Guideline for Implementing Cryptography in the Federal Government
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
SP 800-19	Mobile Agent Security
SP 800-18 Rev. 1	Guide for Developing Security Plans for *Federal* IT Systems
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-16	IT Security Training Requirements: A Role- and Performance-Based Model
SP 800-15 Ver. 1	Minimum Interoperability Specification for PKI Components (MISPC)
SP 800-14	Generally Accepted Principles and Practices for Securing IT Systems
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-12	An Introduction to Computer Security: The NIST Handbook
FIPS 201-1	Personal Identity Verification (PIV) for Federal Employees and Contractors
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 198*-1 (Draft)*	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 197	Advanced Encryption Standard

Publication Number	Title
FIPS 196	Entity Authentication Using Public Key Cryptography
FIPS 191	Guideline for *the* Analysis of LAN Security
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 188	Standard Security Labels for Information Transfer
FIPS 186-*3 (Draft)*	Digital Signature Standard (DSS)
FIPS 185	Escrowed Encryption Standard
FIPS 181	Automated Password Generator
FIPS 180-*3 (Draft)*	Secure Hash Standard (SHS)
FIPS 140-*3 (Draft)*	Security Requirements for Cryptographic Modules
FIPS 113	Computer Data Authentication

CMS continues to work closely with NIST in the development of new standards, FIPS, and security documentation to ensure the highest and most reasonable level of security of Medicare data.

4.1 Security Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FISMA defines three security objectives for information and information systems: confidentiality, integrity, and availability (CIA). FISMA also directs the promulgation of Federal standards for: (i) the security categorization of Federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category. These Federal standards are issued in the form of FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, respectively.

With the passage of FISMA, there is no longer a provision that allows agencies to waive mandatory Federal Information Processing Standards (FIPS). This waiver provision was included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, any references to a "waiver process" contained in any existing FIPS Pub is no longer valid. In addition, OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management, states that government contractors shall abide by FISMA requirements and each agency shall ensure their contractors are doing so.

4.1.1 Potential Security Impact Levels

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FIPS Pub 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or

availability). The application of these definitions shall take place within the context of each organization and the overall national interest.

Table 4.1 defines the three system security levels and their potential security impact.

Table 4.1. System Security Level Definitions

Security Level	*Result*	*Explanation*
High (H)	*Catastrophic Adverse Effect*	• *Severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;* • *Major damage to organizational assets;* • *Major financial loss; or* • *Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.*
Moderate (M)	*Serious Adverse Effect*	• *Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;* • *Significant damage to organizational assets;* • *Significant financial loss; or* • *Significant harm to individuals that does not involve loss of life or serious life threatening injuries.*
Low (L)	*Limited Adverse Effect*	• *Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;* • *Minor damage to organizational assets;* • *Minor financial loss; or* • *Minor harm to individuals.*

4.1.2 Security Levels by Information Type

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS categorized its information according to information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

CMS has defined eleven information types processed by CMS information systems (see Table 4.2 below). For each information type, CMS used FIPS Pub 199 to determine its associated security category by evaluating the potential impact value (e.g., High, Moderate, or Low) for each of the three FISMA security objectives—CIA. The resultant security categorization is the CMS System Security Level. This is the basis for assessing

the risks to CMS operations and assets, and in selecting the appropriate minimum security controls and techniques (i.e., CSRs).

The generalized format for expressing the security category (SC) of an information system is:

SC information system = {(confidentiality impact), (integrity impact), (availability impact)},

where the acceptable values for potential impact are High, Moderate, or Low.

Table 4.2 lists the FIPS Pub 199 security levels for the various information types. The system security level for a FISMA system or application system is determined by its information type(s).

NOTE: In cases where information of varying security levels is combined in a FISMA system or application, the highest security level takes precedence.

Table 4.2. FIPS 199 Security Levels by Information Type

Information Types	Explanation and Examples	System Security Level Security Categorization (SC)
Investigation, intelligence-related, and security information (14 CFR PART 191.5(D))	*Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.*	***HIGH*** *SC={(confidentiality, H), (integrity, H), (availability, M)}*
Mission-critical information	*Information and associated infrastructure directly involved in making payments for Medicare Fee-for-Service (FFS), Medicaid and State Children's Health Insurance Program (SCHIP).*	***HIGH*** *SC={(confidentiality, H), (integrity, H), (availability, H)}*
Information about persons	*Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).*	***MODERATE*** *SC={(confidentiality, M), (integrity, M), (availability, M)}*

Information Types	Explanation and Examples	System Security Level Security Categorization (SC)
Financial, budgetary, commercial, proprietary and trade secret information	*Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payments, payroll, automated decision making, procurement, market-sensitive, inventory, other financially-related systems, and site operating and security expenditures.*	***MODERATE*** *SC={(confidentiality, M), (integrity, M), (availability, M)}*
Internal administration	*Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, advance information concerning procurement actions, management reporting, etc.*	***MODERATE*** *SC={(confidentiality, M), (integrity, M), (availability, M)}*
Other Federal agency information	*Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency.*	***MODERATE*** *SC={(confidentiality, M), (integrity, M), (availability, L)}*
New technology or controlled scientific information	*Information related to new technology; scientific information that is prohibited from disclosure or that may require an export license from the Department of State and/or the Department of Commerce.*	***MODERATE*** *SC={(confidentiality, M), (integrity, M), (availability, L)}*
Operational information	*Information that requires protection during operations; usually time-critical information.*	***MODERATE*** *SC={(confidentiality, M), (integrity, M), (availability, M)}*
System configuration management information	*Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information.*	***MODERATE*** *SC={(confidentiality, M), (integrity, M), (availability, M)}*
Other sensitive information	*Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.*	***LOW*** *SC={(confidentiality, L), (integrity, L), (availability, L)}*
Public information	*Any information that is declared for public consumption by official authorities and has no identified requirement for integrity or availability. This includes information contained in press releases approved by the Office of Public Affairs or other official sources.*	***LOW*** *SC={(confidentiality, L), (integrity, L), (availability, L)}*

4.1.3 CMS Security Level Designation—HIGH

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Although the confidentiality and integrity of some information types (i.e., security category) processed, stored, and/or transmitted on CMS business partner and data center systems could be considered to be at a "Moderate" security level based on the Table 4.2 explanations and examples, CMS has designated all Medicare claims-related information to be "Mission-critical information." Consequently, all CMS business partner and data center information systems shall be designated at a "HIGH" system security level.

Business partner System Managers and System Maintainers/Developers *shall* ensure that their *Medicare claims-related information and information* systems are accessed only by authorized users. The business partner managers of compartmentalized systems *shall* take special care to specify the appropriate level of security required when negotiating with GSSs and MAs for services. The *"HIGH"* security level designation determines the minimum security safeguards required to protect sensitive data and to ensure the operational continuity of *mission*-critical data processing capabilities.

The "HIGH" security level designation applies to both user information and system information, and it is applicable to information in *both digital and* non-*digital* form. System information (e.g., network routing tables, password files, and cryptographic key management information) *shall* be protected at the same level to ensure information and information system confidentiality, integrity, and availability.

4.1.4 Minimum System Security Requirements—HIGH

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FIPS Pub 200 specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. To comply with FIPS Pub 200, agencies shall first determine the security category (i.e., information type) of their information system in accordance with the provisions of FIPS Pub 199, and then apply the appropriate set of baseline security controls contained in NIST SP 800-53 (as amended), Recommended Security Controls for Federal Information Systems. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in NIST SP 800-53. This allows agencies, such as CMS, to adjust the security controls to more closely fit its mission requirements and operational environments.

The CMS Policy for the Information Security Program (PISP) individual policy statements, along with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) required security standards provide technical guidance to CMS and its contractors as to the minimum level of security controls that shall be implemented to protect CMS's information and information systems. These two CMS documents, along with other Federal requirements, form the basis for the CISS CSRs.

4.2 Sensitive Information Protection Requirements

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners are responsible for implementing *the* Minimum Protection Standard*s* (MPS) for all *CMS sensitive* information *(digital and non-digital) and information systems* categorized at *the* "HIGH" security level *designation*. *The MPS establishes a uniform method for protecting data and items that require safeguarding.* The MPS applies to all IT facilities, areas, or systems processing, storing, or transmitting CMS sensitive information *(i.e., any information categorized as "HIGH")* in any form or on any media.

The following table should be used to determine the minimum standards required to protect CMS sensitive information. Note that any of the three alternative protection standards is acceptable whenever all of the applicable perimeter, interior area, and/or container standards are met. The following alternative methods are not listed in any order of preference or security significance.

Table 4.3. *MPS Physical Security*

	Perimeter Type	Interior Type	Container Type
Alternative #1	Secured		Locked
Alternative #2	Locked	Secured	
Alternative #3	Locked		*Security*

Because local factors may require additional security measures, management *shall* analyze local circumstances to determine space, container, and other security needs at individual facilities. The MPS has been designed to provide management with a basic framework of minimum security requirements.

The objective of these standards is to prevent unauthorized access to CMS sensitive information. MPS requires two barriers to accessing sensitive information under normal security *(see Table 4.3).*

"Locked" means a perimeter, area, or container that has both a lock and keys or combinations that are controlled. A secured container is a lockable metal container with a resistance to forced penetration, with both a security lock and keys or combinations that are controlled. (See the following sections for additional explanation and details on these requirements.)

The reason for the two barriers is to provide an additional layer of protection to deter, delay, or detect surreptitious entry. Protected information *shall* be containerized in areas where other than authorized employees may have access after hours (e.g., security personnel or custodial service personnel).

4.2.1 Restricted Area

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A restricted area is a secured area whose entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas *shall* either meet secured area criteria or provisions *shall* be made to store CMS sensitive items in appropriate containers during non-working hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information.

Restricted areas *shall* be indicated by prominently posted signs and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and each entrance *shall* have controlled access (*e.g.,* electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by a responsible employee positioned at the entrance to enforce the restriction of access to authorized personnel accompanied by one or more officials.

4.2.2 Security Room

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A security room is a room that has been constructed to resist forced entry. The primary purpose of a security room is to store protectable material. The entire room *shall* be enclosed by slab-to-slab walls constructed of approved materials (*e.g.,* masonry brick, dry wall, etc.) and supplemented by periodic inspection. All doors for entering the security room *shall* be locked with locking systems meeting the requirements set forth below (section 4.2.5, Locking System*s*). *Entry is limited to specifically authorized personnel.*

Door hinge pins shall be non-removable or installed on the inside of the room. Additionally, any glass in doors or walls *shall* be security glass *(a minimum of* two layers of 1/8-inch plate glass with .060-inch *[*1/32*]* vinyl interlayer, nominal thickness shall be 5/16-inch*)*. Plastic glazing material is not acceptable. Vents and louvers *shall* be protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciate*s* at a protection console, UL-approved central station, or local police station; *and the IDS shall* be given top priority for guard/police response during any alarm situation.

Cleaning and maintenance should be performed in the presence of an employee authorized to enter the room.

4.2.3 *Secured Areas (*Secured Interior / Secured Perimeter*)*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Secured areas are *interior or exterior perimeters which* have been designed to prevent undetected entry by unauthorized persons during non-working hours. To qualify as a *secured* area, the *area shall* meet the following minimum standards:

- Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, or any lesser-type partition supplemented by UL-approved electronic IDS and fire detection systems.

- Unless electronic IDS devices are used, all doors entering the space *shall* be locked and strict key or combination control should be exercised.

- In the case of a fence and gate, the fence *shall* have IDS devices or be continually guarded, and the gate *shall* be either guarded or locked with intrusion alarms.

- The space *shall* be cleaned during working hours in the presence of a regularly assigned employee.

4.2.4 Containers

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving, desk and credenza drawers, carts, *or* any other piece of office equipment designed for the storage of files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide any protection value (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.2.4.1 Locked Container

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A lockable container is a commercially available or prefabricated metal cabinet or box with riveted or welded seams, or metal desks with lockable drawers. The lock mechanism may be either a built-in key, or a hasp and lock.

4.2.4.2 Security Container

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks should have only two keys and strict control of the keys is mandatory. *If c*ombinations *are used, they shall* be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files.

- Metal lateral files equipped with lock bars on both sides and secured with security padlocks.

- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks.

- Key lock “Mini Safes” properly mounted with appropriate key control.

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

4.2.4.3 Safes/Vaults

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A safe/vault is not required for storage of CMS sensitive information. However, if used, *they shall* meet the following requirements:

- A safe is a GSA-approved container of Class *I*, IV, or V, or UL listings of TRTL-30 or TRTL-60.

- A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings that uses UL-approved vault doors and meets GSA specifications.

4.2.5 Locking System*s*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Minimum requirements for locking systems for *s*ecured *a*reas and *s*ecurity *r*ooms are high-security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted deadbolt lock.

- Have a deadbolt throw of one *(1)* inch or longer.

- Double-cylinder design. Cylinders have five *(5)* or more pin tumblers.

- *Contains hardened inserts or inserts made of steel i*f bolt is visible when locked.

- Both *the* key and lock *shall* be “off-master.”

Convenience-type locking devices such as card keys, sequenced button-activated locks used in conjunction with electric strikes, etc., are authorized for use only during working hours. Keys to secured areas not in the personal custody of an authorized employee and *any* combinations *shall* be stored in a security container. *The number of keys or persons with knowledge of the combination to a secured area shall be kept to a minimum.*

4.2.6 Intrusion Detection System*s* (IDS)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Physical Intrusion Detection Systems are designed to detect attempted *breaches of* perimeter area*s*. Physical IDS devices can be used in conjunction with other measures to provide forced entry protection *for* non-working hour *security*. Additionally, alarms for individual and document safety (fire), and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical IDS devices include, but are not limited to: door and window contacts, magnetic switches, motion detectors, and sound detectors, *that* are designed to set off an alarm at a given location when the sensor is disturbed.

5.0 Internet Security

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Transmission of and/or receipt of health care transactions (claims, remittances, etc.) or other CMS sensitive data over the Internet is prohibited at Medicare business partners (or their agents). Practically, this prohibition means that CMS requires the use of private networks or dial-up connections with any entity that transmits or receives health care transactions and/or CMS sensitive data to or from the Medicare contractor. CMS is closely following the health care industry's movement toward adoption of industry-wide security technologies that ensure confidentiality, integrity, and availability of data moved over the Internet and will reconsider its policy at the appropriate time.

Business Partners may use the Internet for: 1) utilizing the IRS Filing Information Returns (FIRE) system by Medicare contractors for Form 1099 submissions, and 2) utilizing e-mail to transmit sensitive information via encrypted attachments in accordance with all applicable CSRs. If not already emplaced, contractors must install firewalls, filtering technology to screen incoming email for high risk transmissions such as executables, up-to-date virus protection software, and intrusion detection software to utilize the Internet.

Appendix A:
The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs)

Table of Contents

(Rev. 9, 06-20-08)

(Rev. 9)

Attachments:

1 – CMS Core Security Requirements (CSR) for High Impact Level Assessments
2 – CMS Core Security Requirements (CSR) for Moderate Impact Level Assessments
3 – CMS Core Security Requirements (CSR) for Low Impact Level Assessments

1 Introduction to the CMS Integrated Security Suite (CISS)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This appendix applies to CMS Business Partners and all other CMS internal/external organizations directed by CMS to use the CISS. CMS Business Partner*s and other entities are* required by CMS *to use the CISS to report the status of Federally- and CMS-mandated security objectives*. *All* CMS-approved Findings from internal *or* external audits *or Federal Information Security Management Act (FISMA) Evaluations shall be* entered into the CISS. *From these Finding entries, Weakness and Action Plan entries shall be generated and* linked with other CISS data as appropriate. This information becomes part of the monthly *Plan of Action and Milestones (*POA&M*)* package as directed in section 3.5.*3* of the BPSSM.

The term "organization" in this appendix applies to all CMS Business Partners and all CMS internal/external information system Business Owners, contractors, sub-

contractors, entities, and their respective employees and facilities supporting CMS business missions.

The mechanics of CISS use are provided in the CISS User Guide, while guidance for populating specific fields is provided in this appendix. The CISS is available for download on the CMS Web site.

2 CISS *FISMA Evaluation* Module

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The annual FISMA Evaluation of controls module functions *in conjunction with the normal Audit/POA&M reporting/tracking process within the CISS*. *For the Annual FISMA Evaluation, organizations* enter text responses to *a subset of the full CMS* Core Security Requirement*s* (CSR)—see Attachment A—indicating the *organization's status towards* compliance with CMS security requirements. In this manner, CMS *organizations* are able to perform their required annual systems security *FISMA Evaluation*s.

The CISS also assists *organizations* by validating and preparing the *FISMA Evaluation* data file for submission to CMS as part of its annual certification material. The CISS *FISMA Evaluation* module provides *organizations* with a powerful reporting tool that generates formatted *FISMA Evaluation* forms, copies of CMS CSRs, and standardized reports.

Organizations shall complete the CISS *FISMA Evaluation* and submit a separate copy for each contract type (i.e. data center, fiscal intermediary, carrier, program safeguard contractor, standard system maintainer, Medicare Administrative Contractor, coordination of benefits, etc.) on CD-ROM to both the CMS Central Office and the Consortium Contractor Management Officer (CCMO) for Title XVIII contracts or the Project Officer (PO) for Federal Acquisition Regulation (FAR) contracts by close of business *on the last business day of* April*, each calendar year* ***except for 2008 when the CISS is due by close of business on August 1, 2008***. *T*his information *may* not be submitted to CMS via email. *Instead,* Registered *M*ail™ or its equivalent *shall* be used. *If* technical assistance *is needed*, contact the CMS/Northrop Grumman Help Desk at 703-272-5725.

The completed *Annual FISMA Evaluation shall* be included in the *organization's* Security Profile (see section 3.7 of the BPSSM). *Organizations* may also use the CISS to conduct *review*s in preparation for audits by specific external entities such as the Government Accounting Office (GAO), Internal Revenue Service (IRS), Department of Health and Human Services (HHS) Office of Inspector General (OIG), and CMS. The CISS *enables organizations* to generate a worksheet consisting of those CSRs and Protocols that have a particular source document as a reference (e.g., IRS Pub 1075, NIST, FISCAM, etc.).

Instructions for using the CISS are contained in the CISS User Guide, which is available in the application itself by clicking on the Help link at the top of the main menu.

2.1 Applicable Laws

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS CSRs detail technical requirements for CMS *organizations that* use information systems to process Medicare data. *Organizations shall* establish and maintain responsible and appropriate controls to ensure the confidentiality, integrity, and availability of Medicare data.

The CMS CSRs are developed by assessing and analyzing requirement statements from a number of Federal and CMS mandates, including the following:

- Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004. http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html

- OMB Circular No. A-127, Financial Management Systems, June 21, 1995. http://www.whitehouse.gov/omb/circulars/index.html

- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999. http://www.whitehouse.gov/omb/circulars/a127transmittal2.html

- *OMB Circular No. A-127, Financial Management Systems, Transmittal 3, December 1, 2004. http://www.whitehouse.gov/omb/memoranda/fy2005/m05-02.html*

- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

- Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000. http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

- *Health Insurance Portability and Accountability Act (HIPAA), August 21, 1996. http://aspe.os.dhhs.gov/admnsimp/pl104191.htm http://aspe.os.dhhs.gov/admnsimp/nprm/sec13.htm*

- *Federal Information Security Management Act of 2002 (FISMA), November 27, 2002. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf*

- Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources, Memorandum, July 17, 2004.
  http://www.whitehouse.gov/omb/memoranda/fy04/m-04-15.pdf

- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, January 1999.
  http://www.gao.gov/special.pubs/12_19_6.pdf

- NIST Special Publication 800-53 *Revision 2*, Recommended Security Controls for Federal Information Systems, *December 2007*.
  http://www.csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

- *NIST Special Publication 800-53A Final Public Draft, Guide for Assessing the Security Controls in Federal Information Systems, December 2007.*
  http://www.csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-A

- CMS *Information Security (IS)* System Security Plans (SSP) *Procedures*, Version *4*.0 *Draft*, *July 10, 2007*.
  http://www.cms.hhs.gov/InformationSecurity

- CMS Information Security Risk Assessment *(IS RA) Procedures*, Version *4.0 Draft*, *July 23, 2007*.
  http://www.cms.hhs.gov/InformationSecurity/Downloads/TBD

- *CMS Policy for the Information Security Program (PISP), CMS-CIO-POL-SEC02-02, November 15, 2007.*
  http://www.cms.hhs.gov/InformationSecurity/Downloads/PISP.pdf

- CMS Information Security *(IS)* Acceptable Risk Safeguards (ARS), Version *3*.0, *September* 1*9*, 200*7*.
  http://www.cms.hhs.gov/InformationSecurity/Downloads/ARS.pdf

- *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities*, *February* 200*7*.
  http://www.irs.gov/pub/irs-pdf/p1075.pdf

2.2 *CMS* CSR *Security Controls*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS CSRs comply with the CMS Policy for Information Security Program (PISP) approach by providing a defense-in-depth security structure along with a least-privilege approach and a need-to-know basis for all information access. The CSRs are not intended to be an all-inclusive list of security controls and are subject to regular updates

to reflect the changing technological environment. The CSRs are not intended to replace a Business Owner's due diligence to incorporate controls to mitigate risk. These controls are the minimum to be considered throughout the risk management process and the System Development Life Cycle (SDLC), and employed where applicable.

The Business Owner, system developer/maintainer, and other internal/external organizations directed by CMS are the target audience for the CSRs. They have primary responsibility for determining the information security requirements and ensuring their implementation. Any organization involved in the SDLC could use this information to understand the baseline information security protections required by CMS.

The CMS CSR security controls in the CISS have a well-defined organization and structure. The security controls are organized into seventeen (17) security control families for ease of use in the control selection and specification process. The security controls in each family are related by their functionality.

The 17 security control families are established by NIST SP 800-53 (as amended), Recommended Security Controls for Federal Information Systems. These security control families are aligned closely with the 17 security-related areas specified in FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

A two-character identifier is assigned to uniquely identify each security control family. Table A-1 summarizes the security control families and the two-character identifier used in the CMS CSRs:

Table A-1. CSR *Security Control Family* Descriptions

Family / Identifier	**Description**
Access Control *(AC)*	*The standards listed in this section focus on how the organization shall limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.*
Awareness and Training (AT)	*The standards listed in this section focus on how the organization shall: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.*
Audit and Accountability (AU)	*The standards listed in this section focus on how the organization shall: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.*

Family / Identifier	Description
Certification, Accreditation, and Security Assessments (CA)	*The standards listed in this section focus on how the organization shall: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.*
Configuration Management (CM)	*The standards listed in this section focus on how the organization shall: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.*
Contingency Planning (CP)	*The standards listed in this section focus on how the organization shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.*
Identification and Authentication (IA)	*The standards listed in this section focus on how the organization shall identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.*
Incident Response (IR)	*The standards listed in this section focus on how the organization shall: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.*
Maintenance (MA)	*The standards listed in this section focus on how the organization shall: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.*
Media Protection (MP)	*The standards listed in this section focus on how the organization shall: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.*
Physical and Environmental Protection (PE)	*The standards listed in this section focus on how the organization shall: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.*

Family / Identifier	Description
Planning (PL)	*The standards listed in this section focus on how the organization shall develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.*
Personnel Security (PS)	*The standards listed in this section focus on how the organization shall: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.*
Risk Assessment (RA)	*The standards listed in this section focus on how the organization shall periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.*
System and Services Acquisition (SA)	*The standards listed in this section focus on how the organization shall: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.*
System and Communications Protection (SC)	*The standards listed in this section focus on how the organization shall: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.*
System and Information Integrity (SI)	*The standards listed in this section focus on how the organization shall: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories, and take appropriate actions in response.*

CMS continues to focus on protecting the health information received from its beneficiaries while processing claims. Ensuring the Confidentiality, Integrity, and Availability (CIA) of CMS sensitive information remains of paramount concern in the continuing effort to improve the overall security program. CMS continually reviews evolving Federal security standards and directives to ensure that the CMS CSRs are current and compliant with all Federal mandates. CMS provides technical clarifications to all organizations and assesses potential impacts of any updated or new requirements. The following rationales are used in preparing these modifications:

- *Where Federal improvements are already covered by an existing CSR, these documents are added as references.*

- *Where Federal improvements are partially covered by an existing CSR, the existing CSR is modified to incorporate appropriate language and the appropriate document(s) are listed as reference(s).*

- *Where Federal improvements are not covered by an existing CSR, a new CSR is added and the appropriate document(s) are listed as a reference(s).*

2.2.1 Security Categorization and Impact Level

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, is the mandatory Federal security categorization standard. It requires organizations to categorize their information systems based on the sensitivity of the information resident on those systems, and the impact on individual operations and assets in the event of a compromise of CIA. The standard is based on the simple and well-established concept of determining information system priorities, and applying reasonable and achievable measures to adequately protect those systems and the data they contain.

FIPS 199 establishes a categorization scheme for information systems as Low-impact, Moderate-impact, or High-impact for the CIA security objectives. The CMS System Security Level is based on the highest value (i.e., high water mark) determined by the CIA for each type of information resident on that information systems. The resultant high water mark is the CMS System Security Level which becomes the basis for selecting appropriate security controls and techniques for protecting CMS operations, assets, and data.

Each security control family contains the applicable security standards with the minimum security controls by security impact level, or in the case of Personnel Security (PS), the position sensitivity level (i.e., High, Moderate, or Low). These standards are designed to assist the Business Owner and system developer/maintainer in defining the information security requirements for their system.

Even though a system may need to be covered by a specific control, the Business Owner may not have to implement that control as long as he/she can demonstrate that the control is satisfied by a higher-level control. The Business Owner assisted by the system developer/maintainer is responsible for evaluating all information security areas within the CSRs and determining the appropriateness for their system.

When a control cannot be implemented even at the minimum level due to resource issues such as funding and personnel constraints or hardware/software limitations, alternative or compensating safeguards can be implemented to reduce the risk to CMS, and CMS

information, information systems, and assets. This shall be considered as part of risk management and the alternative or compensating controls shall be documented in the Information Security (IS) Risk Assessment (RA) and System Security Plan (SSP), and approved by the CMS Chief Information Officer (CIO) or his/her designated representative.

2.2.2 Baseline and Enhancement Security Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

To assist in making the appropriate selection of security controls for information systems, the concept of baseline controls is used. Baseline controls are the minimum security controls recommended for an information system based on the system's security categorization as defined by CMS using FIPS Pub 199. The CMS-tailored baseline security controls (i.e., CMS PISP policy statements) serve as the starting point for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems.

In many cases, enhancement controls are necessary to address specific threats to, and vulnerabilities in, an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., FISMA, HIPAA, IRS, HSPD-7, OMB Circular A-130, Appendix III). Enhancement controls: (i) build in additional, but related, functionality to a baseline control; and/or (ii) increase the strength of a baseline control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment.

Control enhancements are used in supplementing the tailored baselines to achieve the needed level of protection in accordance with a CMS assessment of risk. Moreover, baseline and enhancement controls contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate. Selecting the appropriate set of security controls to meet the specific, and sometimes unique, CMS security requirements is an important task—a task that demonstrates an organization's commitment to security and the due diligence exercised in protecting the CIA of their information and information systems.

The CSR security controls that apply depend upon the mission criticality of the system and its processing environment (e.g., a database on an Internet site as opposed to one on a non-public access mainframe, a General Support System [GSS] vs. a Major Application [MA] system). Another consideration is whether or not the system is covered by higher-level controls, (e.g., an MA that inherits the controls from the GSS on which it operates, or a GSS or MA that inherits the controls of the CMS [or other organization] Master Security Plan).

Three sets of baseline and enhancement controls are included in the CMS CSRs corresponding to the Low-impact, Moderate-impact, and High-impact levels defined in the security categorization process in FIPS 199. Each of the three control sets provide the security controls, including enhancement controls, for a particular impact level associated with a security category.

2.3 CSR *Security Control* Elements

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS CSR security controls are organized into 17 security control families (refer to Table A-1) and each CSR consists of the following elements:

- *CSR Report Assessment Impact Level (i.e., High, Moderate, Low) Identifier*
- *Security Control Family, Identifier, and Class*
- *Baseline/Enhancement Control Number, Name, and Impact Level*
- *Baseline/Enhancement Control*
- *Guidance*
- *Applicability*
- *References*
- *Related Controls*
- *Assessment Procedure*
    - *Assessment Objective*
    - *Assessment Methods and Objects*

All information included in the CSR security control elements is available in the CISS during the FISMA Evaluation process and may be printed from the CISS Reports menu. Table A-2 illustrates a representative layout of the CSR security control elements which are explained in the following sections.

Table A-2. CSR Security Control Element Layout

<table>
<tr><td colspan="3">CMS Core Security Requirements for High Impact Level Assessments
(i.e., CSR Attachment and Assessment Impact Level Identifier)</td></tr>
<tr><td colspan="3">Audit and Accountability (AU) – Technical
(i.e., Security Control Family and Identifier – Security Control Class)</td></tr>
<tr><td colspan="3">AU-6 – Audit Monitoring, Analysis, and Reporting (High)
(i.e., Baseline [or Enhancement] Control Number – Control Name and Impact Level)</td></tr>
<tr><td colspan="3">Control
(i.e., Baseline [or Enhancement] Control Text)

Guidance
(i.e., Supplemental Guidance Text)</td></tr>
<tr><td>Applicability:
(i.e., Applicability Matrix)</td><td>References:
(i.e., Source Documents)</td><td>Related Controls:
(i.e.: Related CSRs)</td></tr>
<tr><td colspan="3">Assessment Procedure: AU-6.1
(i.e., Assessment Procedure section)</td></tr>
<tr><td colspan="3">Assessment Objective
(i.e., Assessment Objectives)

Assessment Methods and Objects
(i.e., Assessment Methods and Objects)</td></tr>
</table>

2.3.1 CSR Attachments and Assessment Impact Levels

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Since CSRs are selected for FISMA Evaluations based upon a system or application CMS security categorization, CSRs are presented by security impact level (High, Moderate, or Low). So, a Moderate impact level assessment contains only the CSRs that apply to Moderate level impact assessments. To accommodate these CSR level differences, there are three (3) attachments to Appendix A:

- *Attachment 1 – CMS CSRs for High Impact Level Assessments*
- *Attachment 2 – CMS CSRs for Moderate Impact Level Assessments*
- *Attachment 3 – CMS CSRs for Low Impact Level Assessments*

Although all three (3) impact levels are stored in the CISS tool, once an assessment impact level is selected, only the selected impact level CSRs are displayed during the FISMA Evaluation process. Likewise, the CISS tool normally prints only the selected impact level CSRs but a capability exists to print other impact level CSRs if desired.

2.3.2 Security Control Family, Identifier, and Class

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS has established three (3) security control classes of information security controls: Management, Operational, and Technical. This structure is consistent with the guidance established by NIST SP 800-53 (as amended).

Management security controls involve those safeguards and countermeasures that manage the security of the information and information systems, and the associated risk to CMS' assets and operations. There are four (4) control families (along with their two-character identifier) within the Management class that address:

1. *Certification, Accreditation, and Security Assessments (CA)*
2. *Planning (PL)*
3. *Risk Assessment (RA)*
4. *System and Services Acquisition (SA)*

Operational security controls support the day-to-day procedures and mechanisms to protect CMS' information and information systems. There are nine (9) control families (along with their two-character identifier) within the Operational class that address:

1. *Awareness and Training (AT)*
2. *Configuration Management (CM)*
3. *Contingency Planning (CP)*
4. *Incident Response (IR)*
5. *Maintenance (MA)*
6. *Media Protection (MP)*
7. *Physical and Environmental Protection (PE)*
8. *Personnel Security (PS)*
9. *System and Information Integrity (SI)*

Technical security controls are those security mechanisms employed within an information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. They are used to authorize or restrict the activities of all levels of users within an individual system by employing access based on a least-privileged and need-to-know approach. There are four (4) control families (along with their two-character identifier) within the Technical class that address:

1. *Access Control (AC)*
2. *Audit and Accountability (AU)*
3. *Identification and Authentication (IA)*
4. *System and Communications Protection (SC)*

Security control families are assigned to their respective security classes based on the dominant characteristics of the controls in that family. Many security controls have

elements logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning (CP) family is listed as an operational control but also has characteristics that are consistent with security management as well.

2.3.3 Baseline and Enhancement Control Number and Name

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

To uniquely identify each baseline control within a security control family (e.g., Audit and Accountability), a one-up sequential number is appended to the family identifier (e.g., AU-1) to indicate the number of the control within the family. For example, AU-6 is the sixth control in the Audit and Accountability family. Additionally, a control name is assigned to the control identifier to identify each security control (e.g., AU-6 – Audit Monitoring, Analysis, and Reporting) within each control family.

To uniquely identify each enhancement control within a security control (e.g., AU-6 – Audit Monitoring, Analysis, and Reporting), a one-up sequential number is appended in parentheses to the control number to indicate the enhancement number within each control. For example, AU-6(1) is the first enhancement control in the AU-6 security control; AU-6(2) is the second, etc.

When the underlying CMS PISP policy statement requires amplification to specify CMS-defined parameters (i.e., assignment and/or selection operations), a "0" in parentheses is appended to the control number [e.g., AC-2(0), AC-7(0)] to indicate a control with CMS-defined control parameters.

While most CMS-tailored enhancement controls map directly to the controls defined in NIST SP 800-53 (as amended), there are some enhancement controls that are unique to CMS and its information systems and/or environment. These CMS-specific tailored controls are included as enhancements within NIST SP 800-53 security control baselines. These enhancements are included within an appropriate security control family (e.g., AC) and security control (e.g., AC-2), and identified using the baseline control number followed by the characters "CMS-" and a sequential number in parenthesis. For example, AC-2(CMS-1) designates the first CMS-specific enhancement to security control AC-2, and AC-2(CMS-2) designates the second.

There are several instances where a CMS-specific enhancement control does not map to an existing baseline control defined in NIST SP 800-53 (as amended). In those cases, a new baseline security control was created within an appropriate existing security control family. These new CMS-specific baseline control include the two-character security family identifier followed by the characters "CMS-" and a one-up sequential number. For example, SC-CMS-1 designates the first new CMS-specific baseline control in the SC security family and SC-CMS-3 designates the third. All enhancement controls to these new CMS-specific baseline controls are then designated using the numbering sequences explained in the previous paragraphs [e.g., SC-CMS-3(CMS-0), SC-CMS-3(CMS-1)].

In addition to CMS-tailored enhancement controls, there are additional security controls that apply to CMS and/or its organizations based on the type of information being stored, accessed, processed, and/or transmitted on their information systems. These enhancements are required by Federal laws, Executive Orders, or directives (e.g., IRS, FISCAM, HSPD-7, HIPAA, CMS-directed requirements).

Some of these additional security controls are already included in existing CMS CSRs, so they do not require separate or additional CSR controls. The security controls that are not already covered by existing CSRs are included as CISS-selectable enhancement controls. For example, FISCAM enhancement controls can be selected (i.e., added) to the CMS minimum baseline controls when required to meet those additional security control requirements. This type of enhancement control includes the standard baseline security control number followed by a unique three-letter character identifier and a one-up sequential number in parentheses. The following three-letter characters identify these additional enhancement controls within the CMS CSRs:

- *DIR – Directed by CMS (includes controls not currently included in the CMS ARS but required by CMS [e.g., PE-3(DIR-1)]*
- *FIS – FISCAM-unique controls [e.g., AC-2(FIS-1)]*
- *IRS – IRS Pub 1075-unique controls required to protect identifiable Federal Taxpayer Information (FTI) [e.g., MP-6(IRS-1)]*
- *PII – Personally Identifiable Information including HIPAA Electronic Protected Health Information [EPHI] this is not unique to HIPAA and/or IRS information that is not identifiable FTI [e.g., AC-20(PII-1)]*

2.3.4 Control

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Control section provides a concise statement of the specific security control capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be performed by the organization or by the information system.

The baseline and enhancement security controls shall be viewed as the foundation or starting point in the selection of adequate security controls for an information system. The security controls represent, for a particular class of information system, the starting point for demonstrating the needed level of security due diligence by an organization in the protection of its operations and assets.

In many cases, enhancement controls are used to supplement baseline controls. Enhancement controls are numbered sequentially within each control so the

enhancements can be easily identified when selected to supplement the basic control. The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements. (Refer to section 2.3.2 above for control numbering.)

The CISS CSRs provide the minimum security controls for information systems, arranged by control families, and selectable by impact level. The CSRs represent the entire set of minimum security controls as defined by CMS at this time.

All CSR baseline security controls are applicable to all organizations unless specifically identified as "Not required" in the CMS CSRs within a specific security level. When a baseline control is "Not required" in the with a specific security level, there will not be any enhancement controls stated for that control identifier.

2.3.5 Guidance

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Guidance section provides supplemental information related to a specific security control when deemed necessary or appropriate. Organizations are expected to apply the guidance as appropriate, when defining, developing, and implementing security controls. In certain instances, the guidance provides more detail concerning the control requirements or important considerations (and the needed flexibility) for implementing security controls in the context of an organization's operational environment, specific mission requirements, or assessment of risk. In addition, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST SPs) are listed in the guidance section, when appropriate, for the particular security control.

2.3.6 Applicability

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All CSRs in a selected control set apply UNLESS a specific contract/entity type is specified as an exception in the Applicability section. Because CMS may add new contract types and/or systems that use the CISS for their FISMA Evaluation, due diligence requires that all security controls be met unless a control is deemed optional for a specific contract/entity type. Refer to the legend below for the current CMS contract types.

Applicability Exception Legend:
ABMAC – A/B Medicare Administrative Contractor
COB – Coordination of Benefits
CWF – Common Working File [Host]
DC – Data Center

DMEMAC – Durable Medical Equipment Medicare Administrative Contractor
EDC – Enterprise Data Center
PartA – Part A Fiscal Intermediary
PartB – Part B Carrier
PSC – Program Safeguard Contractor
QIC – Quality Integrity Contractor
RAC – Recovery Audit Contractor
SS – Standard System [Maintainer]
ZPIC – Zone Program Integrity Contractor

Refer to section 2.4.1 for a brief discussion of the FISMA Evaluation control selection process to the CISS User Guide for instructions on selecting FISMA Evaluation controls.

2.3.7 References
(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The References section identifies the source documents and section or paragraph designations that are the basis or source for the applicable CSR security control. Because the CSRs retain their source references, organizations can conduct "modular" FISMA Evaluations that address the likely audit procedures that would be used by an external audit agency. For example, to prepare for a FISCAM-related audit, an organization's ISSO/SSO might review all the CSRs specifically associated with the FISCAM. In addition, the ISSO/SSO could use references in the CISS database to determine the location of a specific FISCAM requirement.

2.3.8 Related Controls
(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Many, but not all, CSRs may be related to one or more other CSR security control. When addressing some CSRs, it may be important that their responses be consistent with one or more related CSRs. At the very least, organizations shall take care to ensure that related CSR responses do not conflict. While every effort was made to identify related CSRs, other unidentified relationships may exist that are unique to a particular system, contract type, or organization.

2.3.9 Assessment Procedures
(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Assessment Procedures section (i.e., Assessment Objectives, and Assessment Methods and Objects) in the CSRs directly support the validation of individual control effectiveness. The primary objective of the Assessment Procedures is to help determine if the security controls in the information system are effective in their application (i.e., implemented correctly, operating as intended, and producing the desired outcome with

respect to meeting the security requirements of the system). The security Assessment Procedures defined in the CSRs provide a foundational level of assessment to support the security certification process. The Assessment Procedures are identified using their applicable control identifier (e.g., AC-1, AC-2(1), etc.) followed by a numerical decimal identifier (e.g., AC-1.1, AC-2(1).1, etc.)

2.3.9.1 Assessment Objective

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Assessment Procedure consists of a set of procedural steps that are designed to achieve one or more assessment objectives by applying assessment methods to assessment objects.

The Assessment Objectives include a set of determination statements ("Determine if…") related to the particular security control under assessment. The determination statements are closely linked to the content of the security control (i.e., the security control functionality) to ensure traceability of assessment results back to the fundamental control requirements.

Assessment Objectives establish the expectations for security control assessments based on the assurance requirements defined in the security control. The assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness. Each of the Assessment Objective determination statements is either traceable to requirements in the baseline or enhancement security control, or the guidance. This ensures that all aspects of the security control are assessed and that any weaknesses or deficiencies in the control can be identified and remediation actions taken.

NIST SP 800-53A (as amended), Appendix E, Assessment Expectations, provides an explanation of the expectations of security assessments by impact level. These assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness. Organizations are expected to review and use the NIST SP 800-53A assessment expectations as guidance during their FISMA Evaluations.

Table A-3 summarizes the assessment expectations for Low-impact, Moderate-impact, and High-impact information systems.

Table A-3. Assessment Expectations by Information System Impact Level

Assessment Expectations	*Information System Impact Level*		
	Low	*Moderate*	*High*
Security controls are in place with no obvious errors.	√	√	√
Increased grounds for confidence that the security controls are implemented correctly and operating as intended.	–	√	√
Further increased grounds for confidence that the security controls are implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	–	–	√

The decision to reduce the level of effort for the assessment of security controls in Low-impact and Moderate-impact information systems does not affect the basic requirements in the control as stated in the CMS CSRs. The decision to employ optional determination statements and assessment methods shall be a decision guided by an organizational assessment of risk with input from key organizational officials with a vested interest in the assessment and with responsibility for carrying out or supporting CMS missions and business functions.

2.3.9.2 Assessment Methods and Objects

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Assessment Procedure consists of a set of procedural steps that are created to achieve one or more Assessment Objectives by applying assessment methods to assessment objects. As stated in the previous section, the assessment objectives include a set of determination statements related to the particular security control under assessment. The application of assessment procedures to a security control produces assessment findings. These assessment findings are subsequently used in helping to determine the overall effectiveness of the security control.

The three (3) assessment methods defined in the processing component of the framework include Examine, Interview, and Test. NIST SP 800-53A (as amended), Appendix D, Assessment Method Descriptions, provides a detailed explanation of these three (3) assessment methods. Organizations are expected to review and use the NIST SP 800-53A assessment method explanations as guidance during their FISMA Evaluations.

Table A-4 summarizes the hierarchal order of the three (3) assessment methods and their definition.

Table A-4. Assessment Method Hierarchy and Definitions

Assessment Method	Definition
Examine	*The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities) to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.*
Interview	*The process of conducting focused discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.*
Test	*The process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of the security control effectiveness.*

Each of the assessment methods (Examine, Interview, and Test) includes a set of attributes: Depth and Coverage. NIST SP 800-53A (as amended), Appendix D, Assessment Method Descriptions, provides detailed explanations of the assessment method Depth and Coverage attribute values. Organizations are expected to review and use the NIST SP 800-53A assessment method depth and coverage attribute value explanations as guidance during their FISMA Evaluations.

Table A-5 summarizes the assessment method attributes values by information system impact level.

Table A-5. Assessment Method Attributes and Attribute Values by Impact Level

Assessment Methods Examine, Interview, Test	Information System Impact Level		
Attribute	**Low**	**Moderate**	**High**
Depth	*Generalized*	*Focused*	*Detailed*
Coverage	*Representative*	*Specific*	*Comprehensive*

The attribute values for the assessment methods (which describe the rigor and level of detail associated with the assessment) are hierarchical in nature. For the Depth attribute, the Focused attribute value includes and builds upon the assessment rigor and level of detail defined for the Generalized attribute value; the Detailed attribute value includes and builds upon the assessment rigor and level of detail defined for the Focused attribute value. For the Coverage attribute, the Specific attribute value includes and builds upon the number and type of assessment objects defined for the Representative attribute value; the Comprehensive attribute value includes and builds upon the number and type of assessment objects defined for the Specific attribute value.

NIST SP 800-53A (as amended), Appendix E, Assessment Expectations, provides detailed explanations of the assessment objects. Organizations are expected to review and use the NIST SP 800-53A assessment object explanations as guidance during their FISMA Evaluations.

Table A-6 summarizes the assessment objects and their definitions.

Table A-6. Assessment Objects and Definitions

Assessment Object	*Definition*
Specifications	*The document-based artifacts (e.g., policies, plans, procedures, system requirements, designs) associated with an information system.*
Mechanisms	*The specific hardware, software, or firmware safeguards and countermeasures employed within an information system. These also include physical protection devices associated with an information system (e.g., locks, keypads, security cameras, fire protection devices, fireproof safes).*
Activities	*The specific protection-related pursuits or actions supporting an information system that involve people (e.g., system operations, administration, and management; exercises).*
Individuals	*The people or groups of people applying the specifications, mechanisms, or activities described above.*

Recognizing that organizations can specify, organize, document, and configure their information systems in a variety of ways, the assessment objects identified in the CSRs that are provided in conjunction with the Interview, Examine, and Test assessment methods shall be considered suggested objects where information/evidence may be found. As such, assessors are expected to use their judgment in applying the designated assessment methods to the associated set of assessment objects. Each assessment method listed in a procedural step shall be applied to a sufficient number of assessment objects to produce the information necessary to make the determination in the determination statement and to satisfy the assessment objective. It may not always be necessary (or possible) to apply each assessment method to every assessment object in the CSR list.

2.4 Completing the *FISMA Evaluation*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A critical factor for maintaining on-going compliance with FISMA and the Federal Managers' Financial Integrity Act (FMFIA) of 1982, is for Business Owners in coordination with developers, maintainers, and system operators, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing) and person hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of corrective action plans (CAP) for vulnerabilities noted during the testing.

The purpose of annual FISMA Evaluation is to examine and analyze implemented security safeguards in order to provide evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. The annual FISMA Evaluation is intended to test the security controls to determine the extent to which the controls are:

- *implemented correctly,*
- *operating as intended, and*
- *producing the desired outcome with respect to meeting the security requirements for the system.*

The CISS *FISMA Evaluation module* is where *organizations* indicate their compliance with each CSR. *Organizations* select a Status, and provide a descriptive text response that provides details of the Status marked for that CSR.

2.4.1 FISMA Evaluation Control Selection

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The annual FISMA testing requirement has been interpreted by the OMB as being within 365 calendar days of the prior test. Over a three (3) year period, all controls applicable to a system or application shall be tested. This means a subset (no less than one-third [$^1/_3$]) of the security controls shall be tested each year so that all controls are tested during a three (3) year period. This annual subset is inclusive of the required annual test of the system or application Contingency Plan.

While CMS does not mandate which subset of controls shall be tested each year or require a specific number of controls to be tested each year, CMS (and OMB) does require that all controls be tested within a three (3) year period. Business Owners, in coordination with the developer/maintainers of CMS applications and systems, are responsible for meeting this requirement.

The FISMA Evaluation control selection is performed by CISS based on several factors determined through user interview questions/responses. The primary selection factor is the system or application impact level (i.e., High, Moderate, Low). Other selection factors include the type of information handled by the system or application (e.g., PII, FTI) or the source references that apply to the system or application (e.g., FISCAM, IRS). Refer to the CISS User Guide for instructions on selecting FISMA Evaluation controls.

2.4.2 Security Control Assessment

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Security assessments (e.g., FISMA Evaluations) are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits. Rather, they are the last line of defense in the process of identifying the strengths and weaknesses of the organization's information system that supports critical Federal applications and missions in a global environment of sophisticated threats. The findings produced by security assessors during the FISMA Evaluation are used primarily to determine the overall effectiveness of the security controls in an information system, and to provide credible and meaningful inputs to the organization's security accreditation process. A

well-executed security assessment helps to determine the validity of the security controls identified in the information SSP and to facilitate a cost-effective approach to correcting any deficiencies in the system in an orderly and disciplined manner consistent with the organization's mission requirements.

FISMA Evaluations using the assessment procedures (i.e., Assessment Objectives, and Assessment Methods and Objects) provided with each CSR are not intended to make judgments on the necessity or sufficiency of the set of security controls documented in the SSP. Rather the assessment procedures are applied to determine if the security controls employed (and required under CMS policy) within the information system are, in fact, implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Assessors, in the course of executing the procedures within the CSRs, might discover potential errors or oversights in the security plan and shall determine how those potential errors or oversights may affect the CIA of the information system in the event of a compromise or breach of the system. Such discoveries and determinations, however, are a by-product of the assessment and not the purpose of the assessment. Therefore, while assessors are expected to notify appropriate organizational officials about any potential problems with the SSP, assessors are not empowered to second-guess or question the decisions of mission/system owners and authorizing officials concerning the impact level of the information system or the security control selection and supplementation activities, which include the tailoring and supplementation of the security control baselines in the CMS CSRs.

Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling/producing the information necessary to make the determination associated with each assessment objective. Each determination statement in a procedural step contained within an assessment procedure executed by an assessor produces one the following results: (i) Met; or (ii) Not Met. These assessment results are described in Table A-7.

Table A-7. Assessment Results

Level	Description
Met	*Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result.*
Not Met	*Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates potential anomalies in the operation or implementation of the control that may need to be addressed by the organization.*

A result of "Not Met" may also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient evidence to make the particular determination called for in the determination statement. The assessor results (i.e., the determinations made) shall be an objective reporting of what was found concerning the

security control assessed. For each assessment result of other than "Met," assessors shall indicate which parts of the security control are affected by the finding (i.e., those aspects of the control that were deemed not met or were not able to be assessed) and describe how the control differs from the planned or expected state. Any potential for compromises to confidentiality, integrity, and availability due to a "Not Met" finding shall also be noted by the assessor.

The assessor results are aggregated and documented for each control requirement in the CISS FISMA Evaluation (refer to the CISS User Guide) and they serve as a primary information source for the POA&M. The assessor does not prepare the POA&M, but may provide recommendations for its content. The Business Owner may have an opportunity to address some or all of the weaknesses or deficiencies in the security controls identified during the assessment before those weaknesses or deficiencies become part of the POA&M. However, senior leadership involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in some priority order—first providing resources to the information systems that are supporting the most critical and sensitive missions for the organization. Each identified Finding and corresponding Weakness shall be addressed with a corrective Action Plan in the CISS before submission of the FISMA Evaluation to CMS.

Ultimately, the assessment results and any subsequent mitigation actions initiated by the Business Owner in collaboration with designated organizational officials trigger updates to the IS RA and the SSP. Therefore, the key documents used by the authorizing official to determine the security status of the information system (i.e., SSP with updated IS RA, security assessment report, and POA&M) are updated to reflect the results of the security assessment.

2.5 All *CSR* Responses

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The following information and guidance *shall* be considered when evaluating all CSRs and preparing *FISMA Evaluation* CSR responses *in the CISS*:

a) Each CSR *response* requires a *compliance* Status (i.e., *Met*, *Not Met, or Not Applicable [N/A]*) to be selected, *accompanied by* a detailed explanation in the Response Comment/Explanation field *that provides* a complete description of What, Where, Why, and How each CSR *element* is or is not *met*.

b) A reference to the applicable section, page, or paragraph of the FISMA Evaluation working papers where the applicable Assessment Procedure was performed and documented. (A single copy of the FISMA Evaluation working papers shall be attached electronically the FISMA Evaluation Audit/Review record in the CISS Tool.)

c) Every CSR response requires that a principle Point-of-Contact (POC) be designated. The CISS provides a specific field for this information, and the field requires that at least one POC value be entered. Other interested POCs may also be assigned to a CSR as non-primary designees. However, one and only one primary POC *shall* be assigned to each CSR response.

d) *Organization*s should be aware that even if data processing duties are subcontracted out to either another CMS *organization* (such as a data center) or to a third-party subcontractor (such as a business services company), responsibility for the implementation *and evaluation* of security controls ultimately resides with the primary contract holder. *Organization*s *shall* coordinate the establishment of boundaries for specific issues. While this does not necessarily require a sharing of *FISMA Evaluation* responses, it does require that *organization*s communicate and coordinate among themselves such that interfaces of responsibilities for particular CSRs are addressed by all responsible *organizations* without gaps in coverage.

e) Where a merging of responsibilities occurs among *organization*s (such as the interface between data centers, claims processors, and standard system maintainers), a detailed description of these interfaces and the division of responsibilities *shall* be provided in the Response Comment/Explanation field. The description *shall* include local responsibilities as well as those that are perceived to be responsibilities of some other CMS *organization*.

f) Each CSR in the CISS includes an Applicability *section*, which identifies *those* CMS contract*/entity types* (i.e., Part A, Part B, CWF, etc.) *where specific CSRs may not apply*. The purpose of the Applicability *section* is not to summarily exclude CSRs from a particular contract*/entity* type. The Applicability *section* is designed to be used as a guide. CMS recognizes that system configurations vary widely throughout the *CMS* community; therefore, each *organization shall* evaluate and report on each CSR's applicability to its own systems.

g) *Organization*s should also be aware of the CSR terms included in the BPSSM Glossary (Appendix H) and address the CSRs as they apply to their local environment. For example, the term "data center" *(i.e., computer facility) is defined as "*a site or location *with computer hardware* where information process*ing is performed"* (e.g., claims entry and processing)*. This term* is not limited to *any specific* CMS *Enterprise* Data Center *(EDC) or Carrier/FI Data Center* environment. A "system" may include mainframe systems, desktop systems, workstations and servers, networks, and any platform regardless of the operating system. "System software" includes the operating system and utility programs (e.g., workstation, server, and network software and utilities) and is distinguished from application software. "Application software" includes the standard system (i.e., *MA*) but it also includes any computer program (i.e., application) that manipulates data or performs a specific function (e.g., front-end and back-end applications).

h) If *organizational* policy conflicts with a CMS CSR, a detailed explanation *shall* be provided as to why the *organization* policy cannot be modified to apply to CMS data. Any conflicts with *organization* policy (in which the final disposition of the CSR response would not ultimately result in full compliance with CMS requirements) *shall* be addressed for resolution, by written correspondence with the CMS Central Office, prior to indicating *such a non-compliance status* in any CSR response.

*Organization*s are required to enter a current *compliance* status *(Met, Not Met, N/A)* and a detailed Comment/Explanation for each CSR. The annual *FISMA Evaluation* is one of the central *security* documents in *an organization*'s security profile and *shall* reflect sufficient detail to convey to CMS the current status of the *organization*'s security program.

2.6 *"Not Applicable" (*N/A*)* Response Status

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A response status of "N/A" indicates that the *CSR security control* requirements *may* not *be* applicable to th*e organization*. CMS expects most, if not all, CSRs to apply to all portions of all *CMS* contracts *and expects all CSRs to be evaluated as to their applicability*. Very few CSRs are expected to receive "N/A" responses. The Response Comment/Explanation field *shall* contain a detailed explanation of the circumstances that render this CSR non-applicable (regardless of whether this CSR is listed as *not* applicable in *A*pplicability matrix for a particular contract type), and how this information can be verified, in a format that clearly answers each question described below:

a) **Why** is this CSR not applicable?

   A complete and detailed description *shall* be provided to describe the circumstances that render the subject CSR "N/A" to a particular *organization*. Referral to the Applicability matrix is NOT sufficient justification for an "N/A" response. A full understanding of the reasons for non-applicability *shall* be demonstrated and explained in the CSR response. This is *necessary* because the Applicability matrix is not definitive, and CMS anticipates cases in which a CSR will indeed apply to one or more *organizations* even when the CISS Applicability matrix indicates it generally does not. CMS approvals (and the citation[s] thereof) are not required for "N/A" responses that are corroborated by the CISS Applicability *matrix*.

b) **How** did you verify this status with CMS?

   i. **Applicability matrix *indicates* CSR is NOT applicable.** CMS approvals (and the citation[s] thereof) are not required for "N/A" responses that are corroborated by the CISS Applicability matrix. *However, an explanation is required amplifying why the organization agrees that the CSR is "N/A."*

ii. **Applicability matrix *indicates* CSR is applicable.** In the case of an "N/A" response that is not corroborated by the Applicability matrix, CMS approval *shall* be obtained and documented, and such documentation *shall* be provided with the CSR response (see below). Note that CMS approval must be renewed each year for each "N/A" CSR *that is not corroborated by the Applicability matrix*.

iii. ***Conditional CSR.*** *A conditional CSR is a control prefixed with a conditional "If" statement (e.g., "If automated information labeling is utilized…" or "If wireless access is explicitly approved…"). For conditional CSRs where the conditional control is not required to be used or implemented (i.e., automated information labeling is not used), a "Met" response, with an explanation detailing that the required preconditions do not exist, is appropriate.*

The CISS requires that copies of the associated CMS approval documentation *be* attached to the CSR response within the CISS tool. Approvals for prior years may be cited in request*s* for CMS approval for the current year response but *prior year approvals* cannot be used as documentation of CMS approval for the current year CSR "N/A" response. Each year, the CMS approval process *shall* be repeated (unless specifically stated *otherwise* in the CMS-provided approval documentation).

In addition to the requirements stated above in section 2.6.a), include the following information with *each* CMS-approved "N/A" response:

(1) Date CMS approved the response,
(2) CMS office that approved the response, and
(3) Attached documentation of CMS concurrence (e-mail text file, or letter/document).

2.7 *Compliance Status*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Testing of the CSR compliance will result in one of two FISMA compliance control status: "Met" or "Not Met." Other than the "N/A" response (which indicates that the control requirement is not required) explained in Section 2.6, "Met" and "Not Met" are the only CSR status responses available in the CISS to report a FISMA Evaluation result. To determine compliance, the CSR Assessment Procedures provided with each CSR shall be applied to determine if the security controls as employed within the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the applicable security requirement.
As stated previously, baseline controls are the minimum security controls recommended for an information system based on the system's security categorization. Enhancement

controls provide additional, but related, functionality to a baseline control; and increase the strength of the baseline control. Although each baseline and enhancement control is assessed separately and its compliance status is recorded separately, the CISS does not allow a baseline control group (e.g., AC-1, AC-2, AC-3, etc.) to be fully compliant unless all of the control group enhancements are also compliant [e.g., AC-2(1), AC-2(2), AC-2(3), etc.]. The CISS automatically determines overall control group compliance and provides feedback when a control group is not compliant (refer to the CISS User Guide for additional information).

The decision tree in Figure A-1 has been developed to help organizations establish their CSR compliance status for each baseline and enhancement control.

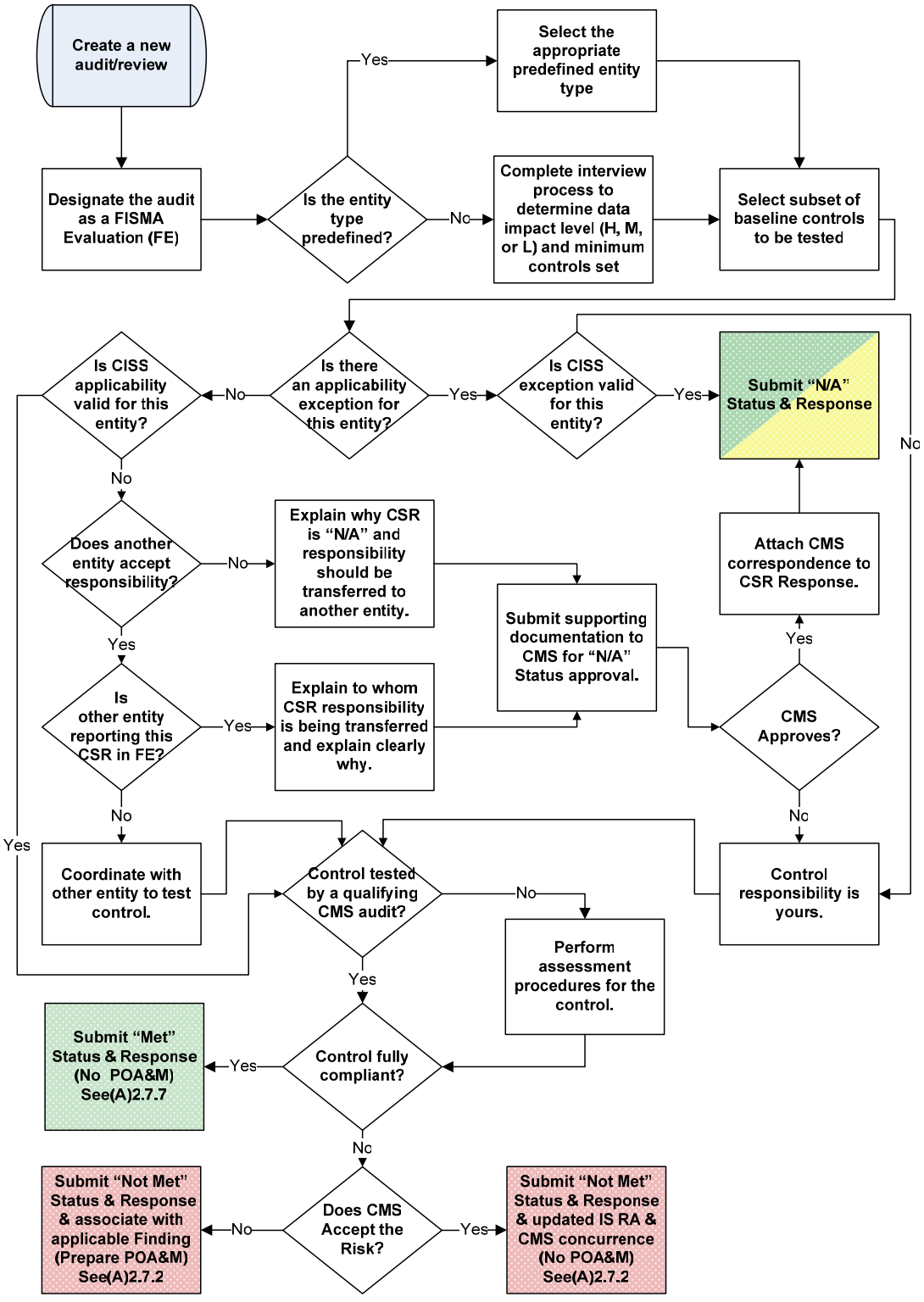

Figure A-1. Response Status Decision Tree

2.7.1 *"Met"* Response Status

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Response Comment/Explanation field *shall*, at a minimum, contain a detailed explanation of how the stipulations of the CSR are being met, and how compliance can be verified, in a format that clearly answers each question described below:

a) ***Who*** *performed the evaluation?*

Each CSR response shall include a reference to the applicable Audit/Review in which the applicable CSR was tested. From this reference, the entity that performed the Evaluation of the applicable control may be determined. Within the CISS, the default Audit/Review will be the current FISMA Evaluation. However, other qualifying Audit/Reviews may be referenced (such as a qualifying SAS 70, or other audit.) If another qualifying management-directed audit/review performed the applicable CSR Assessment Procedures (or their equivalent), those results may be used as support for the current FISMA Evaluation. In this case, the Assessment Procedures do not need to be repeated.

All management-directed and independent testing conducted within 365 days of the attestation due date may be used to meet the requirement for annual security controls testing. Management-directed and independent testing includes:

- *Certification and Accreditation (C&A) independent ST&E testing,*
- *OMB Circular A-123 IT EDP assessment,*
- *Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) Section 912 evaluations,*
- *MMA Testing,*
- *Statement on Auditing Standard (SAS) 70 reviews,*
- *Certification Package for Internal Controls (CPIC) audits,*
- *General Accounting Office (GAO) reviews,*
- *FE testing, and*
- *Testing results from local test teams (i.e., organizationally separated from the Medicare operations team) organized for purposes of meeting this requirement.*

Testing pursuant to the Chief Financial Officer (CFO) audit of CMS financial statements cannot be used. CFO testing is directed by the Office of the Inspector General (OIG) and is not considered management-directed.

b) **What** can be used to verify full compliance?

*While not required to be included as supporting documentation in the FISMA Evaluation submission, d*ocumentation in the form of *policies, procedures,* manuals, employee training records, *and logs shall* be available to verify compliance. *A description of these documents shall be included in the*

Comment/Explanation field. The control *shall be tested using the CSR Assessment Procedures (i.e., Assessment Objective, and Assessment Methods and Objects) to verify compliance*. *All* document*ation specified in the CSR shall* be *verified* for a response to be considered complete.

c) **Where** can the applicable *evaluation* documentation be found?

Verification of the performance of the applicable Assessment procedures for each CSR is a fundamental part of the FISMA Evaluation process. Methods of verification *in accordance with the applicable CSR Assessment Procedures* should be accessible to *reviewers*. Ensure that *a cross reference to section/page/paragraph in the working papers of the applicable audit/review documentation* is clearly described. *The applicable referenced working papers shall also be provided with the overall FISMA Evaluation. If another audit or review is cited as the source of testing, applicable working papers for the referenced audit/review shall also be included (electronically) with the FISMA Evaluation submission*.

d) **How** exactly *are* the CSR *assessment objectives being* met?

i. Do not include planned controls or controls that are not fully implemented. If all components are not fully in place, the response status *shall* be changed to *"Not Met"* and a suitable Weakness/Action Plan combination identified.

ii. In some cases, alternative controls might be implemented to achieve the intent of the CSR. Ensure that information about implementation of alternative controls to meet the specifics of the applicable CSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.

To be effective, *FISMA Evaluations shall* include tests and examinations of security controls. *The evaluations shall be conducted using the applicable Assessment Procedures.*

2.7.2 "Not Met" Response Status

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A response status of "Not Met" implies that the assessment information obtained during the evaluation indicates potential anomalies in the operation or implementation of the control that will need to be addressed by the organization. A status of "Not Met" may also indicate that for reasons specified in the assessment report (and entered in the CSR Response), the assessor was unable to obtain sufficient evidence to make the particular determination called for in the determination statement (i.e., Assessment Objectives).

For each assessment status of "Not Met," assessors shall indicate which parts of the security control are affected by the assessment finding (i.e., those aspects of the control that were deemed not met or were not able to be assessed) and describe how the control differs from the planned or expected state, and this information shall be entered in the applicable CSR Response Comment/Explanation field.

A "Not Met" CSR status results in one of the following:

a) ***Finding.*** *The status of each CSR baseline and enhancement shall be fully compliant or "Met." For any response status that is not compliant, the [Finding] button on the CISS FISMA Evaluation form is enabled. An appropriate Finding (and associated Weakness)/Action Plan combination shall accompany any CSR response that is "Not Met."*

b) ***Risk-Based Decision.*** *In extremely rare cases, full compliance of a CSR minimum security requirement may present unacceptable fiscal or configuration barriers. In such cases, CMS may agree that the risk is acceptable for the present and no Finding/Action Plan combination is required or desired. In such cases, prior CMS concurrence is required AND a full assessment of all of the implications of not being in full compliance of the minimum security requirements for the applicable CSR is fully documented in the associated system IS RA. BOTH the updated IS RA AND full documentation of CMS concurrence SHALL be attached to the CSR response.*

2.8 Findings and Weaknesses

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Weaknesses form the basis for CISS Action Plans (see section 2.9 of this appendix for a description of Action Plans). *Audit* Findings*, which include FISMA Evaluation* non-compliant CSR *Finding*s*,* form the basis of Weaknesses.

Every Finding *shall* be addressed by a Weakness record in the CISS. A Finding is any deficiency identified and reported during an audit or review—whether internal or external. For example:

> "Login accounts exist for employees who have left the company."

A Weakness, in this context, would be the underlying cause for, or source of, the Finding. For example:

> "No policy exists for the removal of accounts when employees leave."

A FISMA Evaluation Finding can be associated with one or more non-compliant CSRs but only if the security controls or assessment findings are related. A Weakness *shall* be

identified for each Finding*; h*owever, a single Weakness may address several Findings. Consider the following simplified illustration:

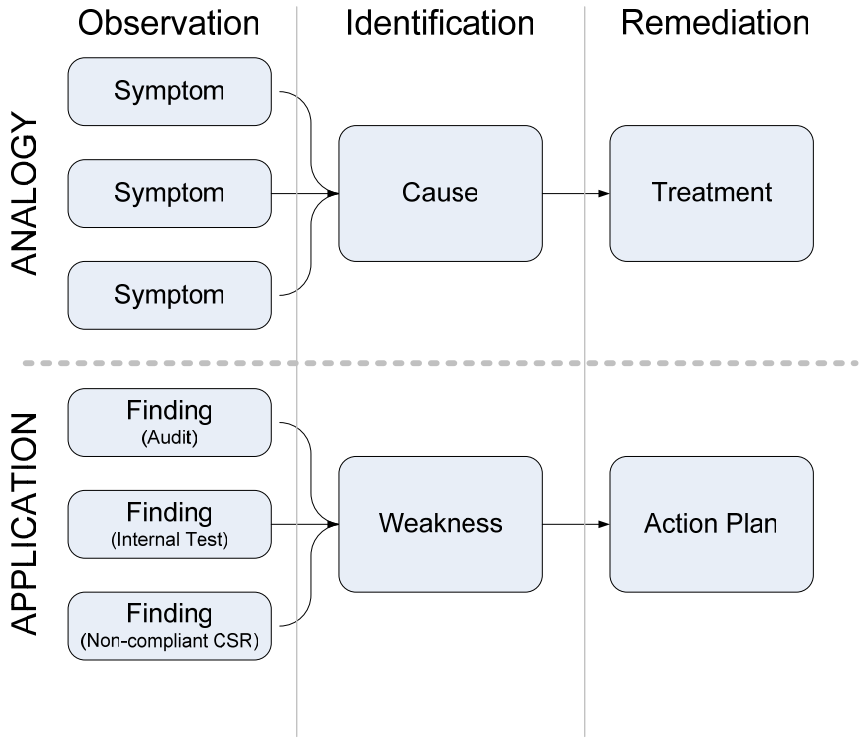

Figure A-2. Analogy for Finding-Weakness-Action Plan Relationship

An Action Plan *shall* be designated to address each Weakness.

Weaknesses that need to be recorded and tracked can be identified either reactively or proactively. Reactive Weakness determination indicates that outside auditors or reviewers identified Findings leading to the Weakness determination. Proactive Weakness determination occurs by conducting regular program and system reviews using *FISMA Evaluation*s or internal reviews. Sources of security-related Findings and Weaknesses include, but are not limited to:

- Chief Financial Officer (CFO)/Electronic Data Processing (EDP) Audits related to annual CFO Financial Statement Audits (which may include network vulnerability assessment/security testing *[*NVA/ST*]*)
- Statement on Auditing Standards No. 70 (SAS 70) Audits
- Submission of a Certification Package for Internal Controls (CPIC)
- HHS OIG IT Controls Assessment
- Financial reviews conducted by the General Accounting Office (GAO)

- Section 912 Evaluations or Testing
- Data *C*enter *S*ystem *T*ests
- Penetration/External Vulnerability Assessment (EVA) *T*ests
- *FISMA Evaluation*s
- *Information Security* Risk *A*ssessments
- Internal or *S*elf-directed *R*eviews, *A*udits, or *T*ests

This list is not exhaustive; there are many avenues for discovering Weaknesses. In the CISS, a*ll Findings and* Weakness*es are* considered to have resulted from some type of audit or review.

The flow in Figure A-3 has been developed to assist organizations establish the linkage among Findings, Weaknesses, and Action Plans.

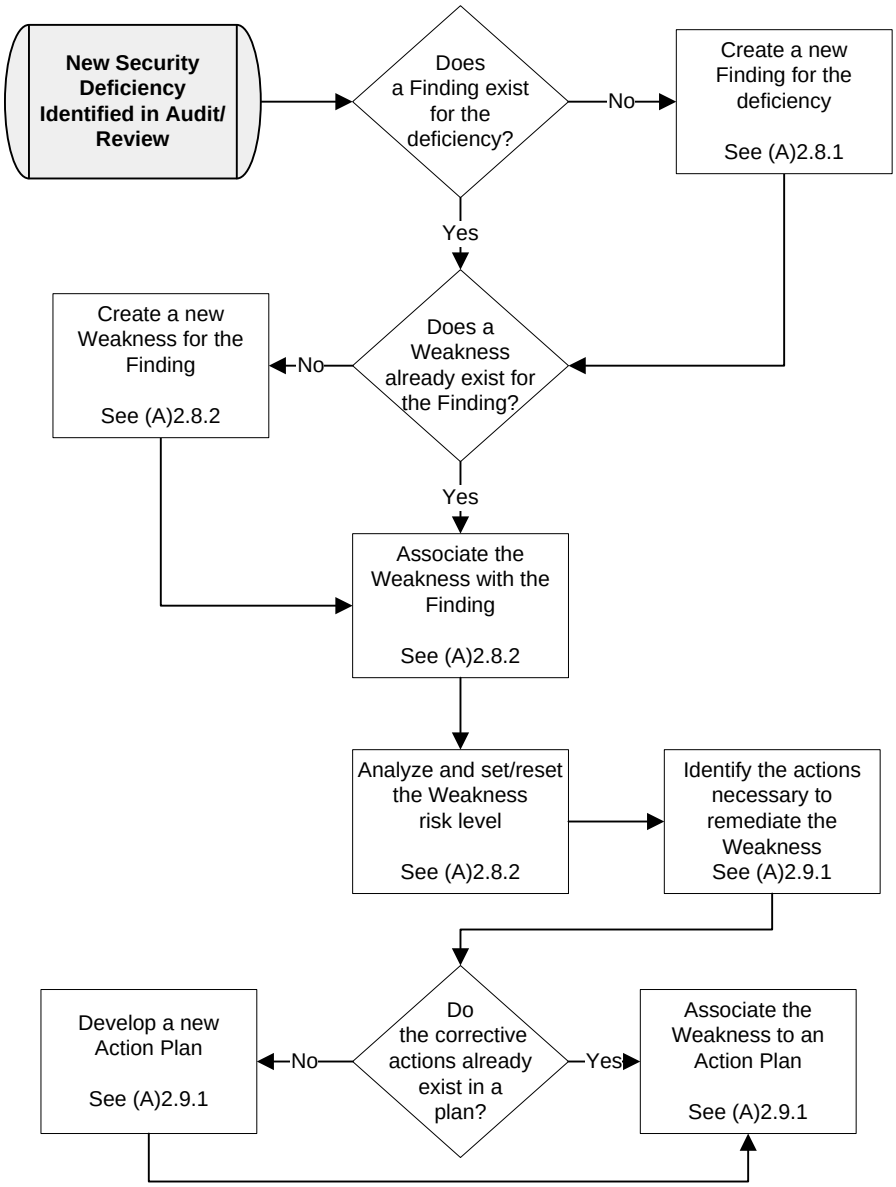

Figure A-3. Weakness Decision Tree

2.8.1 Findings

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All security-related Findings identified or reported by internal or external audits and reviews *shall* be entered into the CISS and associated with (i.e., linked to) one Weakness.

The following subsections provide guidance for populating the CISS Findings form. Consult the CISS User Guide for specific instructions related to accessing and working with CISS Findings form components.

2.8.1.1 Finding Identifier

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Finding identifier is normally the same identifier provided in the audit or review report. If an internal Finding is identified, the Finding is recorded by a unique identifier consisting of the following information:

a) **Entity.** The first three *(3) to five (5)* characters identify the name of the contractor. These *entity-identifiers* are listed under contractor abbreviations in Chapter 7, Internal Control Requirements, section 40.3, CMS Finding Numbers, of the Medicare Financial Manual (CMS Pub 100-6).

NOTE: This unique *entity*-identifier is not reported to agencies outside of CMS nor is it included in CMS' annual or quarterly POA&M submissions to OMB. Findings reported outside CMS cannot be traced to a *CMS organization or contractor*.

b) **Year.** The next four *(4)* digits denote the Fiscal Year (FY) in which the Finding was identified and first reported. The year is normally the same as assigned in the audit or review report.

c) **Code.** The next one *(1)* or two *(2)* characters identifies the type of review or audit. They are as follows:

9E	*Section 912 Evaluation*
9T	*Section 912 Testing*
A	*A-123 Non-IT Assessment*
AT	*Authority to Operate*
C	*CPIC, (Your annual self certification package)*
CA	*Certification and Accreditation*
CP	*Contingency Plan*
DR	*CFO Desktop Review*
E	*CFO EDP Review*
F	*CFO Financial Review*
FE	*FISMA Evaluation*
G	*GAO Reviews (Financial Reviews)*
I	*A-123 IT (EDP) Assessment*
IR	*Internal reviews initiated by the entity to meet other Federal requirements*
M	*CMS CPIC Workgroup Reviews*
N	*SAS 70 Novation*
O	*OIG Reviews (HHS Office of Inspector General [IT] Controls Assessment)*
P	*CMS 1522 Workgroup Reviews*
R	*Accounts Receivable Review*
RA	*Risk Assessments*
S	*Statement on Auditing Standards No. 70 (SAS 70)*
SP	*System Security Plan*

V CFO Related NVA/ST

d) **Num.** The next three *(3)* digits are the sequential Finding number assigned to each individual Finding beginning with 001, 002, 003, etc. The number is normally the same as assigned in the audit or review report.

2.8.1.2 Finding Title and Description

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Finding title *shall* not include any contractor-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the contractor reporting the Finding, or the location, facility, system, or application to which the Finding refers. Some appropriate Finding titles might include: "inadequate password controls," "insufficient or inconsistent data integrity controls," "inadequate firewall configuration reviews," "background investigations not performed prior to system access," "insufficient physical access controls," etc.

The intent is to provide a title that is descriptive but does not reveal sensitive or exploitable information, such as: "Telnet port open, allowing access by outside users." The title *shall* also be unique enough to be more readily identifiable by name than by number. The Finding title reported in the audit or review report *shall* generally be used, unless that title is too long or contains sensitive descriptive information.

The Finding description *shall* be the descriptive Finding information reported in the audit or review report. This description is not reported beyond CMS, so there is no restriction on its content. If the Finding is the result of an internal audit or review, the description *shall* include the Finding information required by the GAO, "Government Auditing Standards," GAO-03-673G (http://www.gao.gov/govaud/yb2003.pdf), commonly referred to as the "Yellow Book."

2.8.1.3 Finding Status

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All security-related Findings *shall* include a status that indicates the stage or state of the Finding corrective action. Since a Weakness may be associated with multiple Findings, one or more Findings associated with the Weakness can be closed while the Weakness remains open. The four *(4)* Finding status reporting choices are:

- **On-going.** The Finding remains open and action is on-going to correct it. However, if the Initial Target Completion Date entered in the Action Plan has passed and action is still on-going to correct the Weakness, the status *shall* be reported as Delayed.

- **Closed Pending.** (1) If the Finding was discovered in an internal review, the *organization may* proceed directly to the Closed status. (2) If the Finding was reported by a CMS initiated audit or review, the *organization* should use this status when it considers the Finding closed. However, CMS requires this type of Finding closure to be validated before it is considered Closed. The *organization* should continue to report the status as Closed Pending until the closure is validated and CMS provides documentation confirming the Closed status. The CISS will require that appropriate documentation be attached to this status to confirm the closure. This documentation *shall* address all aspects of the stated Finding and be sufficient for CMS validation of closure.

- **Closed.** If a Finding has been officially closed by CMS*, with supporting documentation as proof submitted* to the *organization*, it should be reported as Closed in the CISS. The CISS will require that appropriate missing or updated documentation not previously sent be attached to this Closed status to confirm the closure. This documentation *shall* also include any CMS closure letters.

- **Delayed.** Action is on-going to correct the Finding but the Initial Target Completion Date entered in the Action Plan has passed. The Finding should continue to be reported as Delayed until the Finding is corrected and reported as closed.

2.8.1.4 Determination of Finding Risk Level

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FISMA guidance requires that all Weaknesses be prioritized to ensure that significant IT security Weaknesses take precedence and are immediately mitigated. Since a Finding indicates a Weakness, a risk level *shall* also be assigned to each Finding.

System Finding risk levels should be determined in the system's risk assessment. The risk level determination process is the same for both Findings and Weaknesses and is summarized in section 2.8.2.9, Determining Risk.

2.8.1.5 Finding FMFIA and CPIC Severity

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Findings, and their associated Weaknesses, *shall* be disclosed as Material Weaknesses or Reportable Conditions if they have an impact on the contractor's internal control structure. Every Finding identified as an internal control deficiency should be categorized as either a Material Weakness or a Reportable Condition based on the following definitions:

- A **Reportable Condition** exists when the internal controls are adequate in design and operation and reasonable assurance can be provided that the intent of the

control objective is met, but deficiencies were found during the review that requires correction.

- A **Material Weakness** exists when the contractor fails to meet a control objective. This may be due to a significant deficiency in the design and/or operation of internal control policies and procedures. Because of these shortfalls in internal controls, the contractor cannot provide reasonable assurance that the intent of the control objective is being met.

2.8.1.6 Finding *Security Control Family*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All Findings *shall* be assigned to one of the *CMS Security Control Families*. These *families* are available from a drop-down menu in the CISS.

2.8.1.7 Finding Point(s) of Contact

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

For each Finding reported, a primary POC *shall* be selected. While multiple POCs can be assigned to a Finding, only one POC can be designated as primary for each Finding. The primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the Finding. Non-primary POCs can include anyone who will assist the primary POC in resolving the Finding.

2.8.2 Weaknesses

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All security-related Weaknesses identified by internal or external audits and reviews, including *FISMA Evaluation*s, *shall* be entered into the CISS and associated with (i.e., linked to) an Action Plan AND one or more Findings.

The following subsections provide guidance for populating the CISS Weakness form. Consult the CISS User Guide for specific instructions related to accessing and working with CISS Weakness form components.

2.8.2.1 Weakness Identifier

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Each Weakness *shall* be identified and recorded by a unique identifier consisting of the following information:

a) **Entity.** The first three *(3) to five (5)* characters identify the name of the contractor. These contractor *identifiers* are listed under contractor abbreviations in Chapter 7, Internal Control Requirements, section 40.3, CMS Finding Numbers, of the Medicare Financial Manual.

   NOTE: This unique contractor identifier is not reported or included in CMS' annual or quarterly POA&M submissions. Therefore, Weaknesses reported outside CMS cannot be traced to a *CMS organization or contractor* by any information included in the Weakness identifier.

b) **Quarter.** The next single character represents the FY quarter in which the Weakness was first identified and entered into the POA&M, where:

   A = 1st Quarter
   B = 2nd Quarter
   C = 3rd Quarter
   D = 4th Quarter

c) **Year.** The next four *(4)* digits are the FY in which the Weakness was identified and first reported.

d) **Number.** The next number is incremental, representing the sequence in which the Weakness was entered into the contractor's POA&M.

For example, a Weakness identified as "CMS_B_2005_3" indicates this CMS Weakness was identified and first reported during the 2nd quarter of FY 2005, and it is the 3rd Weakness identified during that time period.

2.8.2.2 Weakness Title and Description

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Weakness title *shall* not include any contractor-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the contractor reporting the Weakness, which location or facility has the Weakness, or what system or application has the Weakness.

The intent is to provide a title that is descriptive but does not reveal sensitive or exploitable information. The title *shall* also be unique enough to be more readily identifiable by name than by number.

The Weakness description, however, is not reported beyond CMS, and it *shall* provide sufficient information and detail to allow CMS to evaluate the Weakness.

2.8.2.3 Weakness *Security Control Family*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All Weaknesses *shall* be assigned to one of the *CMS Security Control Families*. These *families* are available from a drop-down menu in the CISS:

2.8.2.4 Determination of Weakness Risk Level

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

System Weakness risk levels should be determined in the system's risk assessment according to criteria in the CMS *IS* RA *Procedures*.

2.8.2.5 Weakness FISMA Severity

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FISMA requires the reporting of any significant deficiency in a policy, procedure, or practice to be identified as a material Weakness under the Federal Managers Financial Integrity Act (FMFIA), and if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (FFMIA). Depending on the risk and magnitude of harm that could result, Weaknesses identified during the review of security controls are reported as deficiencies in accordance with OMB Circular No. A 123, “Management Accountability and Control,” and FMFIA.

Although the CISS includes the three *(3)* FISMA Severity levels listed below, only one *(1)* level is activated and available for use by *organizations* (i.e., Weakness). The other two *(2)* severity levels, Significant Deficiency and Reportable Condition, require that CMS make a risk-based decision before a Weakness can be assigned to them. Should CMS make that determination, additional guidance will be provided on how to select a different severity level.

The three *(3)* FISMA Severity levels are:

- **Weakness.** The term Weakness refers to any and all other IT security Weaknesses pertaining to the system.

  NOTE: This is the only severity level that can be selected by *organizations* at this time.

- **Reportable Condition.** A Reportable Condition exists when a security or management control Weakness does not rise to a significant level of deficiency; yet, it is still important enough to be reported to internal management. A security Weakness may be considered a Reportable Condition even though it is not deemed to be a Significant Deficiency by agency management if it affects the

efficiency and effectiveness of agency operations. However, due to lower risk, corrective action may be scheduled over a longer period of time.

- **Significant Deficiency**. A Significant Deficiency exists when a Weakness in an agency's (i.e., CMS) overall information systems security program or management control structure, or within one or more information systems, significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies *shall* be notified and immediate or near-immediate corrective action *shall* be taken.

2.8.2.6 Weakness Type

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

There are two *(2)* types of security-related Weakness that *shall* be identified:

- **Program Weakness.** A Program Weakness impacts multiple IT systems as a result of a deficiency in the IT security program.

- **System Weakness.** A System Weakness pertains to the management, operation, or technical controls of a specific IT system.

2.8.2.7 Weakness Status

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All security-related Weakness corrective actions *shall* include a status that indicates the stage or state of the Weakness corrective action. Since multiple Findings may be associated with a Weakness, the Weakness cannot be closed until all Findings associated with it are closed. The five *(5)* Weakness status reporting choices are:

- **On-going.** The Weakness remains open and action is on-going to correct it. However, if the Initial Target Completion Date entered in the Action Plan has passed and action is still on-going to correct the Weakness, the status *shall* be reported as Delayed.

- **Closed *Pending*.** *(1) If the Weakness was discovered in an internal review, the organization may proceed directly to the Closed status.* (2) If the Weakness was discovered in an outside audit or review, the *organization* should use this status when it considers the Weakness closed. However, CMS requires this type of Weakness closure to be validated before it is considered closed. The contractor should continue to report the status as Closed *Pending* until the closure is validated.

- **Closed.** If a Weakness has been officially closed by *CMS, with supporting documentation as proof submitted to the organization, it should be reported as Closed in the CISS.*

- **Delayed.** Action is on-going to correct the Weakness but the Initial Target Completion Date entered in the Action Plan has passed. The Weakness should continue to be reported as Delayed until the Weakness is corrected and reported as closed.

2.8.2.8 Weakness Point(s) of Contact

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

For each Weakness identified, a primary POC *shall* be selected. While multiple POCs can be assigned to a Weakness, only one POC can be designated as primary for each Weakness. The primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the Weakness. Non-primary POCs can include anyone who will assist the primary POC in resolving the Weakness.

2.8.2.9 Determining Risk

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The risk determination process explained in this section is taken from the CMS IS RA *Procedures*. The process described here assumes that specific threats and vulnerabilities have already been identified. Consult the CMS IS RA *Procedures* for specifics on identifying threats and vulnerabilities.

While both system and business risk measurements are discussed and combined in the CMS IS RA *Procedures* document, risk determinations made in and by the CISS are for systems only. The goal of risk determination is to calculate the level of risk for each threat/vulnerability pair based on:

1. The likelihood of a threat exploiting a vulnerability; and

2. The severity of impact that the exploited vulnerability would have on the system, its data and its business function in terms of loss of CIA.

2.8.2.9.1 Likelihood of Occurrence

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The risk likelihood level is determined by considering known threats as they may apply to known system vulnerabilities. The likelihood is an estimate of the frequency or the probably of such an event. The likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access, and existing controls; the presence, motivation, tenacity, strength, and nature of the threat; the presence of vulnerabilities; and the effectiveness of existing controls.

Refer to the information in Table A-*8* for guidelines to determine the likelihood of occurrence that a threat is realized and exploits the system's vulnerability.

Table A-*8*. Likelihood of Occurrence Levels

Likelihood	Description
Negligible	Unlikely to occur.
Very Low	Likely to occur two *(2)*/three *(3)* times every five *(5)* years.
Low	Likely to occur once every year or less.
Medium	Likely to occur once every six *(6)* months or less.
High	Likely to occur once per month or less.
Very High	Likely to occur multiple times per month.
Extreme	Likely to occur multiple times per day.

2.8.2.9.2 Impact Severity

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The severity of impact is the magnitude or severity of impact on the system's operational capabilities and data if the threat is realized and exploits the associated vulnerability. The severity of impact for each threat/vulnerability pair is determined by evaluating the potential loss in each security category (CIA) based on the system's information security level as explained in BPSSM Section 4.0, Information and Information Systems Security. The impact can be measured by loss of system functionality, degradation of system response time, or inability to meet a CMS business function, dollar losses, loss of public confidence, or unauthorized disclosure of data.

Refer to Table A-*9* for guidelines to determine system impact severity levels.

Table A-*9*. System Impact Severity Levels

Impact Severity	Description
Insignificant	Will have almost no impact if threat is realized and exploits vulnerability.
Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
Serious	May cause considerable system outage, and/or loss of connected

Impact Severity	Description
	customers or business confidence. May result in compromise or large amount of Government information or services.
Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.

2.8.2.9.3 *Determining the* Risk *Level*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The overall risk level can be expressed in terms of the likelihood of the threat exploiting the system vulnerability and the impact severity of that exploitation on the CIA of the system. This overall level of risk is depicted in the following equation:

Risk Level = Likelihood of Occurrence *X* Impact Severity

After the risk likelihood of occurrence and impact severity have been established, the overall level of risk is determined using the following risk level matrix (Table A-*10*). The level of risk equals the intersection of the likelihood of occurrence and impact severity values. The CISS determines this value automatically based on the input values of the Weakness likelihood of occurrence and impact severity selections.

Table A-*10*. Overall Risk Level Matrix

Likelihood of Occurrence	Impact Severity					
	Insignificant	Minor	Significant	Damaging	Serious	Critical
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

2.9 Action Plans and POA&Ms

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Action Plans form the basis for the periodic POA&M reporting requirement (see section 3.5.2 of the BPSSM for reporting requirements).

The CISS assists *organizations* in reporting Weaknesses, preparing Action Plans, and submitting the required POA&Ms to CMS. The POA&M submission process is

automatic in that it contains information already entered into the CISS. Therefore, no further guidance is required beyond the instructions found in section 11, Submissions to CMS, of the CISS User Guide. The remainder of this section is devoted to guidance for populating the CISS Action Plan form.

2.9.1 Completing Action Plans

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Each Weakness entered into the CISS *shall* correspond to an Action Plan for its resolution. Although the CISS does permit multiple Weaknesses to be addressed by a single Action Plan, this approach is not recommended, because a Weakness cannot be closed until its corresponding Action Plan has been completed.

Corrective action methods should be analyzed for appropriateness in fully resolving any associated Weakness; they should also be viewed for long-term implications. When completing an Action Plan, the cost for each option *shall* be estimated and analyzed to determine short- and long-term solution capabilities.

2.9.1.1 Action Plan Title and Description

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Action Plan title *shall* not include any contractor-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the contractor reporting the Weakness, which location or facility has the Weakness, or what system or application has the Weakness. The title is used only to provide a descriptive name to the Action Plan so it can be distinguished from other Action Plans.

Detailed descriptions of Action Plans are necessary, and sufficient text is required to permit oversight and tracking. Sensitive information *shall* not be revealed in the description of the Action Plan, Weakness, or associated Milestones. In addition, no contractor-, location-, or system-specific information *shall* be included in the Action Plan description. Otherwise, the descriptive information can be used to identify the contractor, location or facility, or system or application.

2.9.1.2 Determining Completion Dates

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Completion Dates (i.e., Initial Target, Current Projected, and Actual) are populated automatically based on dates entered in the Milestones. These dates will change based on the Milestone dates until the Action Plan is reported in a POA&M submission. Once the Action Plan has been initially submitted to CMS, the Initial Target date is locked and cannot be changed. So, when completing Milestones, completion dates *shall* be determined based on realistic timelines for resources to be obtained and associated steps to be completed. For example, although it may take 30 days to complete the required Action Plans for a specific Weakness, it may not be possible to complete ALL Action

Plans for all Weaknesses during the same time period due to staffing resource limitations. Therefore, the Initial Target Milestone dates *shall* be based on the outcome of prioritization decisions and resource availability.

2.9.1.3 Determining Costs

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

In determining Weakness remediation costs, *organizations shall* consider the following criteria to determine security costs for a specific IT investment:

a) The products, procedures, and personnel (*organization* employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. This includes the costs of:

- Risk assessment
- Security planning and policy
- Certification and accreditation
- Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
- Authentication or cryptographic applications
- Education, awareness, and training
- System reviews/evaluations (including security control testing and evaluation)
- Oversight or compliance inspections
- Development and maintenance of *organization* reports to CMS and corrective Action Plans as they pertain to the specific investment
- Contingency planning and testing
- Physical and environmental controls for hardware and software
- Auditing and monitoring
- Computer security investigations and forensics
- Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations

b) Security costs *shall* also include the products, procedures, and personnel (*organization* employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; system administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.

c) Many corporate entities operate networks that provide some or all of the necessary security controls for the associated applications. In such cases, the *organization shall* nevertheless account for security costs for each application investment. To avoid “double-counting,” *organizations* should appropriately

allocate the costs of the network for each of the applications for which security is provided.

In identifying security costs, *organizations* may find it helpful to ask the following simple question: "If there were no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" If *organizations* encounter difficulties with the above criteria, they *shall* contact CMS prior to submission of their POA&M report.

Target Implementation Costs are the total costs for implementing the remediation safeguards during the first year of implementation. This *shall* include purchases, leases, setup and delivery, consultant services, applicable overhead, depreciation, amortization, cost of money, and all other associated costs in accordance with disclosure practices. Since this cost may be used for budgetary purposes, it *shall* be as accurate as feasible. It is advised that finance, accounting, or other personnel familiar with the application of cost estimating practices be consulted when estimating this cost.

The Estimated Annual Maintenance cost is the projected recurring cost of implementing the remediation safeguards. This is the projected recurring cost to CMS to maintain this remediation safeguard for the following FY. This cost *shall* include depreciation, amortization, etc. Costs associated with continued funding should be added to subsequent line one charges where applicable.

The Percent Security value is the percentage of the total remediation safeguard costs that pertain or apply to security.

The Percent Applied to CMS is the percentage of the total remediation safeguard cost being charged to CMS. This is the percentage of cost that CMS will fund for safeguards that will be shared between CMS (Medicare) systems and corporate systems.

2.9.1.4 Determining Funding Sources

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CISS requires that some resources be identified for every Action plan. Action Plans cannot be executed without the application of resources (personnel or procurement). Therefore, the CISS will not accept "zero-cost" Action Plans. Resources for Weakness remediation can be obtained through the following means:

- Using current resources marked for security management of the system or program. This *shall* be the method used for resourcing most Weaknesses.

- Reallocating existing funds or personnel.

- Requesting additional funding.

Requesting new or additional funding from CMS to remediate a Weakness should only be used when no other source of funding can be identified. When funding is available, CMS will prioritize funding allocations based on Weakness prioritization and risk levels. It is in the *organization*'s best interest to use current resources or reallocate existing funds or personnel to remediate all Weaknesses. All funding reallocations *shall* be approved by CMS.

2.9.1.5 Milestone Title and Description

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Milestone title *shall* not include any sensitive or identifying information. The title *shall* be descriptive enough to distinguish one Milestone from another.

Detailed descriptions of Milestones are not necessary, but sufficient data is required to permit oversight and tracking. Sensitive or identifying information *shall* not be revealed in the Milestone descriptions.

2.9.1.6 Milestones with Completion Dates

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Fundamentally, the Action Plan is simply a container for the Milestones that address remediation of any corresponding Weakness. The Milestones are identified in the POA&M, and each one *shall* correspond to a specific corrective action. Ideally, there *shall* be at least one Milestone per quarter so that Action Plan progress can be tracked in the POA&M submissions to CMS.

Including anticipated completion dates with each Milestone enables progress toward Weakness mitigation to be tracked. Each Milestone within the POA&M *shall* include an anticipated date of completion (Projected Date). Once Milestones and completion dates are entered, changes can be made until the Action Plan is first submitted.

The overall projected completion date of the Action Plan is derived automatically by the CISS based on the projected completion dates of all of the Milestones. The Initial Target date remains unchanged once the Action plan has been submitted to CMS. However, the Current Projected Date will adjust automatically based on changes in milestone projected completion date. (Note that the Action Plan status of “Delayed” is always calculated based on the Initial Target date.)

Milestones should effectively communicate the major steps within an Action Plan that *shall* be performed to mitigate a Weakness. For example, appropriate Milestones for an Action Plan associated with a Weakness such as “Identification and authentication process need to be more stringent” might read:

- Evaluate methods for strengthening identification and authentication
- Develop procedures to standardize accepted authentication process
- Acquire management approval/sign-off of new process and procedures
- Implement approved authentication process

2.9.1.7 Milestone Changes

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

If a situation exists that prevents a Milestone and/or overall corrective action from being completed on time, the new estimated date of completion will automatically be reflected in the Current Projected date based on the Milestone changes. However, once the Action Plan has been submitted, the Initial Target date field is locked and cannot be changed. Any changes to a Milestone *shall* include the reason(s) for the delay.

Business Partners Systems Security Manual

Appendix A, Attachment 1

CMS Core Security Requirements (CSR)

for

High Impact Level Assessments

CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

Rev. 9

(This page intentionally left blank)

Access Control (AC) – *Technical*

AC-1 – Access Control Policy and Procedures (High)

Control

Logical access controls and procedures shall be established and implemented effectively to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (i.e., programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

Guidance

The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AC-1; FISCAM: TAC-3.2.C.1, TAC-4.3.4, TSD-1.1.1, TSD-2.1, TSS-1.1.1; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1; NIST 800-53/53A: AC-1; PISP: 4.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents access control policy and procedures;
(ii) the organization disseminates access control policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review access control policy and procedures; and
(iv) the organization updates access control policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.
Interview: Organizational personnel with access control responsibilities.

ASSESSMENT PROCEDURE: AC-1.2

Assessment Objective

Determine if:
(i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.
Interview: Organizational personnel with access control responsibilities.

AC-1(FIS-1) – Enhancement (High)

Control

Standard forms are used to document approval for archiving, deleting, or sharing data files. Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

Applicability: All	**References:** FISCAM: TAC-2.3.1, TAC-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-1(FIS-1).1

Assessment Objective

Determine if:
(i) the organization uses standard forms to document approval for archiving, deleting, or sharing data files; and
(ii) the organizational agreements, with other entities, document prior to sharing data or programs how the data files are protected.

Assessment Methods And Objects

Examine: Documents authorizing file sharing and file sharing agreements.
Examine: Pertinent policies and procedures.
Examine: Standard approval forms.
Interview: Data owners.

AC-2 – Account Management (High)

Control

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. Access to the CMS information system shall be granted based on: (a) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (b) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

Guidance

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

Applicability: All	**References:** ARS: AC-2; FISCAM: TAC-3.2.C.4, TAC-3.2.C.5, TSP-4.1.6, TSS-1.1.3; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2.1

Assessment Objective

Determine if:
(i) the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts;
(ii) the organization defines the frequency of information system account reviews;
(iii) the organization reviews information system accounts at the organization-defined frequency, at least annually; and
(iv) the organization initiates required actions on information system accounts based on the review.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing account management; information system security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.
Interview: Organizational personnel with account management responsibilities.

AC-2(0) – Enhancement (High)

Control

Review information system accounts every 90 days and require annual certification.

Applicability: All	**References:** ARS: AC-2(0); FISCAM: TAC-3.2.C.4, TSS-1.1.4; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records.
Interview: Organizational personnel with account management responsibilities.

AC-2(1) – Enhancement (High)

Control

Employ automated mechanisms to support the management of information system accounts.

Applicability: All	**References:** ARS: AC-2(1); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to support information system account management functions.

Assessment Methods And Objects

Examine: Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.

AC-2(2) – Enhancement (High)

Control

Configure the information system to allow emergency account for a period of time NTE 24 hours and to allow accounts with a fixed duration (i.e., temporary accounts) NTE 365 days.

Applicability: All	**References:** ARS: AC-2(2); FISCAM: TAC-2.2; IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(2).1

Assessment Objective

Determine if:

(i) the organization defines a time period after which the information system terminates temporary and emergency accounts; and

(ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.

Assessment Methods And Objects

Examine: Information system security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.

AC-2(3) – Enhancement (High)

Control

Configure the information system to disable inactive accounts automatically after 90 days.

Applicability: All	**References:** ARS: AC-2(3); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(3)	**Related Controls:** IA-4(0)

ASSESSMENT PROCEDURE: AC-2(3).1

Assessment Objective

Determine if:

(i) the organization defines a time period after which the information system disables inactive accounts; and

(ii) the information system automatically disables inactive accounts after organization-defined time period.

Assessment Methods And Objects

Examine: Procedures addressing account management; information system security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.

AC-2(4) – Enhancement (High)

Control

Employ automated mechanisms to audit user account creation, modification, disabling, and termination. Ensure the automated mechanism notifies appropriate personnel of the user account management actions.

Applicability: All	**References:** ARS: AC-2(4); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(4)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(4).1

Assessment Objective

Determine if:

(i) the organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions; and

(ii) the organization employs automated mechanisms to notify, as required, appropriate individuals.

Assessment Methods And Objects

Examine: Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.

AC-2(CMS-1) – Enhancement (High)		
Control Remove or disable default user accounts. Rename active default accounts.		
Applicability: All	**References:** ARS: AC-2(CMS-1); FISCAM: TAC-3.2.A.3, TAC-3.2.C.4, TSS-1.2.3; IRS-1075: 5.6.3.2#2.1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(CMS-1).1		
Assessment Objective Determine if the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. **Assessment Methods And Objects** **Examine:** Access control policy and procedures; other relevant documents or records to determine if the organization removes or disables default user accounts. It must also rename active default accounts if they must be used. **Interview:** Organizational personnel with access control responsibilities to determine that all default user accounts are either removed or disabled. If default accounts are active, that they are renamed. **Test:** Information system sample of hosts with defined users to ensure that all default user accounts are either removed or disabled. If default accounts are active, that they are renamed.		
AC-2(CMS-2) – Enhancement (High)		
Control Require the use of unique and separate administrator accounts for administrator and non-administrator activities.		
Applicability: All	**References:** ARS: AC-2(CMS-2); FISCAM: TAN-2.1.4; IRS-1075: 5.6.3.2#2.1	**Related Controls:** IA-4(CMS-1)
ASSESSMENT PROCEDURE: AC-2(CMS-2).1		
Assessment Objective Determine if the information system enforces separation of duties through assigned access authorizations. **Assessment Methods And Objects** **Examine:** Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if the organization prohibits administrator accounts to be used for day-to-day activities. **Interview:** Organizational personnel with account management responsibilities to determine if administrator accounts are being used for day to day activities. **Test:** Information system sample of hosts' system logs to ensure that administrator accounts are not being used for day-to-day activities.		
AC-2(CMS-3) – Enhancement (High)		
Control Implement centralized control of user access administrator functions.		
Applicability: All	**References:** ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(CMS-3).1		
Assessment Objective Determine if the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. **Assessment Methods And Objects** **Examine:** Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if all user access administrator functions are centralized. **Interview:** Organizational personnel with account management responsibilities to determine if all user access administrator functions are carried out by a centralized administrator function. **Test:** Information system sample of hosts' system logs to determine if all user access administrator functions are carried out by a centralized administrator function.		
AC-2(CMS-4) – Enhancement (High)		
Control Regulate the access provided to contractors and define security requirements for contractors.		
Applicability: All	**References:** ARS: AC-2(CMS-4); IRS-1075: 5.6.3.2#2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(CMS-4).1

Assessment Objective

Determine if the organization documents contractor security requirements and maintains contractor access privileges.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if all contractors' access are authorized, regulated, and security requirements for contractors are defined.

Interview: Organizational personnel with account management responsibilities to determine if written authorizations exist for a sample of contractor employees.

AC-2(CMS-5) – Enhancement (High)

Control

Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked prior to or during the termination process.

Applicability: All	**References:** ARS: AC-2(CMS-5); FISCAM: TSP-4.1.6; IRS-1075: 5.6.3.2#2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(CMS-5).1

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine when employee access rights are revoked on termination.

Interview: Organizational personnel with personnel security responsibilities to determine when access is revoked on employee termination.

AC-2(FIS-1) – Enhancement (High)

Control

All system access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to security managers.

Guidance

The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties.

Applicability: All	**References:** FISCAM: TAC-2.1.1, TAC-2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(FIS-1).1

Assessment Objective

Determine if:

(i) the organization grants system access authorizations on standard forms and maintains the completed forms on file; and

(ii) the organizational senior managers approve system access authorizations and the approvals are securely transferred to security managers.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Selection of user (both application user and information system personnel) access authorization documentation.

Interview: Personnel involved in access authorizations and senior managers who approve authorizations.

AC-2(FIS-2) – Enhancement (High)

Control

Business Owners periodically review system access authorization listings and determine whether they remain appropriate. ISSO/SSOs review system access authorizations and discuss any questionable authorizations with Business Owners.

Applicability: All	**References:** FISCAM: TAC-2.1.2, TAC-2.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(FIS-2).1

Assessment Objective

Determine if the organizational ISSO/SSOs periodically reviews system access authorization listings and discusses questionable authorizations with management.

Assessment Methods And Objects

Examine: Access authorization listings to determine whether inappropriate access are removed in a timely manner.

Examine: Pertinent policies and procedures.
Interview: Business Owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner.
Interview: ISSO/SSOs and review documentation provided to them.

AC-3 – Access Enforcement (High)

Control

Access enforcement mechanisms shall be developed, documented and implemented effectively to control access between named users (or processes) and named objects (e.g., files and programs) in a CMS information system. Additional application level access enforcement mechanism shall be implemented, when necessary, to provide increased information security for CMS information. When encryption of stored information is employed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (see section 4.16.13).

Guidance

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

Applicability: All	**References:** ARS: AC-3; FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.C.6, TAC-3.2.D.1, TCC-3.2.3, TSS-2.1.1, TSS-2.1.2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3; NIST 800-53/53A: AC-3; PISP: 4.1.3	**Related Controls:** MA-CMS-1, MA-CMS-2, SC-13

ASSESSMENT PROCEDURE: AC-3.1

Assessment Objective

Determine if:
(i) the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy; and
(ii) user privileges on the information system are consistent with the documented user authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing access enforcement policy.

AC-3(1) – Enhancement (High)

Control

Ensure the information system restricts access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.

Guidance

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Applicability: All	**References:** ARS: AC-3(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.2, TAC-3.2.C.5, TAC-3.2.D.1, TCC-3.2.3, TSD-3.1.4, TSS-1.1.2, TSS-2.1.2; IRS-1075: 5.6.3.2#2.2; NIST 800-53/53A: AC-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-3(1).1

Assessment Objective

Determine if:
(i) the organization explicitly defines privileged functions and security-relevant information for the information system;
(ii) the organization explicitly authorizes personnel access to privileged functions and security-relevant information in accordance with organizational policy; and
(iii) the information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel (e.g., security administrators).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing access enforcement policy.

AC-3(CMS-1) – Enhancement (High)		
Control If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).		
Applicability: All	**References:** ARS: AC-3(CMS-1); IRS-1075: 5.6.3.2#2.2	**Related Controls:** SC-13
ASSESSMENT PROCEDURE: AC-3(CMS-1).1		
Assessment Objective Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. **Assessment Methods And Objects** **Examine:** Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if encryption is used as an access control mechanism, examine system and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13). **Interview:** Organizational personnel with access control responsibilities to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13). **Test:** Information system if encryption is used as an access control mechanism; examine organization's encryption key lengths, algorithms, certificates, etc.		
AC-3(CMS-2) – Enhancement (High)		
Control If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix A for e-Authentication Standards.		
Applicability: All	**References:** ARS: AC-3(CMS-2); IRS-1075: 5.6.3.2#2.2	**Related Controls:**
ASSESSMENT PROCEDURE: AC-3(CMS-2).1		
Assessment Objective Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users). **Assessment Methods And Objects** **Examine:** Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if e-authentication is used as an access control mechanism, examine Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the organization's encryption standard meets ARS Appendix A for e-Authentication Standards. **Interview:** Organizational personnel with access control responsibilities if e-authentication is used as an access control mechanism, interview system administrators responsible for the hosts providing authentication services to determine if the organization meets the standards described in ARS Appendix A. **Test:** Information system if e-authentication is used as an access control mechanism; test a sample of hosts for automated mechanisms implementing identification and authentication capability for the information system.		
AC-3(CMS-3) – Enhancement (High)		
Control Configure operating systems controls to disable public "read" and "write" access to all system files, objects, and directories. Configure operating system controls to disable public "read" access to files, objects, and directories that contain sensitive information.		
Applicability: All	**References:** ARS: AC-3(CMS-3); FISCAM: TAC-3.2.D.1, TCC-3.2.3; IRS-1075: 5.6.2.3#1, 5.6.3.2#2.2	**Related Controls:**
ASSESSMENT PROCEDURE: AC-3(CMS-3).1		
Assessment Objective Determine if the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements. **Assessment Methods And Objects** **Examine:** Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive		

information.

Interview: Organizational personnel with access control responsibilities to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

Test: Automated mechanisms implementing access enforcement policy to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

AC-3(CMS-4) – Enhancement (High)

Control

Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas.

Applicability: All	References: ARS: AC-3(CMS-4); FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.D.1, TAY-3.1.6, TCC-3.2.3; HIPAA: 164.312(a)(2)(iv); IRS-1075: 5.6.3.2#2.2	Related Controls:

ASSESSMENT PROCEDURE: AC-3(CMS-4).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if data stored in the information system is protected with system access controls and must be encrypted when residing in non-secure areas.

Interview: Organizational personnel with access control responsibilities to determine if hosts storing data are protected with system access controls and if data stored in non-secure areas are encrypted.

Test: Automated mechanisms implementing access enforcement policy to if data stored on these hosts is protected with system access controls and that it is encrypted if residing in non-secure areas.

AC-4 – Information Flow Enforcement (High)

Control

Flow control shall be enforced over information between source and destination objects within CMS information systems and between interconnected systems based on the characteristics of the information.

Guidance

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

Applicability: All	References: ARS: AC-4; IRS-1075: 5.6.3.2#2.2; NIST 800-53/53A: AC-4; PISP: 4.1.4	Related Controls: SC-7

ASSESSMENT PROCEDURE: AC-4.1

Assessment Objective

Determine if the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information flow enforcement policy.

ASSESSMENT PROCEDURE: AC-4.2

Assessment Objective

Determine if interconnection agreements address the types of permissible and impermissible flow of information between information systems and the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system interconnection agreements; information system configuration settings and associated

documentation; list of information flow control authorizations; information system audit records; other relevant documents or records.

AC-5 – Separation of Duties (High)

Control

The principle of separation of duties shall be enforced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission functions and distinct information systems support functions shall be divided among different roles, and support functions shall be performed by different individuals (e.g., personnel responsible for administering access control functions shall not also administer audit functions). Personnel developing and testing system code shall not have access to production libraries. Access control software shall be in place to limit individual authority and information access, such that the collusion of two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties.

Guidance

The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Applicability: All	References: ARS: AC-5; FISCAM: TAY-1.3.2, TSD-1.1.1, TSD-1.1.2, TSD-1.1.3, TSD-1.1.5, TSD-1.2.1, TSD-1.3.3, TSD-2.2.2, TSS-1.1.2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3; NIST 800-53/53A: AC-5; PISP: 4.1.5	Related Controls:

ASSESSMENT PROCEDURE: AC-5.1

Assessment Objective

Determine if:
(i) the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and
(ii) the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing separation of duties; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records.
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties.
Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-1) – Enhancement (High)

Control

Ensure that audit functions are not performed by security personnel responsible for administering access control.

Applicability: All	References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5	Related Controls:

ASSESSMENT PROCEDURE: AC-5(CMS-1).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if audit functions are NOT performed by security personnel responsible for administering access control. Also, ensure that the organization enforces separation of duties through assigned access authorizations.
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are NOT performed by security personnel. Also, determine if access authorizations complement and reinforce separation of duties.
Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-2) – Enhancement (High)

Control

Maintain a limited group of administrators with access based upon the users' roles and responsibilities.

Applicability: All	References: ARS: AC-5(CMS-2)	Related Controls:

ASSESSMENT PROCEDURE: AC-5(CMS-2).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization maintains a limited group of administrators with access based upon the users' roles and responsibilities.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the number of personnel with root access is limited to only those personnel with a business need for root access.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-3) – Enhancement (High)

Control

Ensure that critical mission functions and information system support functions are divided among separate individuals.

Applicability: All	**References:** ARS: AC-5(CMS-3); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-3).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-4) – Enhancement (High)

Control

Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Applicability: All	**References:** ARS: AC-5(CMS-4); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-4).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-5) – Enhancement (High)

Control

Ensure that an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.

Applicability: All; Optional for SS	**References:** ARS: AC-5(CMS-5); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-5).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the

information system, conducts information security testing of the information system.
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties. None of these individuals or functions should be conducting information security testing of the information system.
Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-6) – Enhancement (High)

Control

Ensure that quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions are conducted by an independent entity, not the code developers.

Applicability: All	**References:** ARS: AC-5(CMS-6); FISCAM: TSD-1.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-6).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions are conducted by an independent entity, not the code developers.
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if coders do their own quality assurance or code reviews.
Test: Automated mechanisms implementing separation of duties policy.

AC-5(FIS-1) – Enhancement (High)

Control

Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.

Applicability: All	**References:** FISCAM: TSD-1.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(FIS-1).1

Assessment Objective

Determine if the organization provides adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Interview: Personnel to determine whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.

AC-6 – Least Privilege (High)

Control

Each user or process shall be assigned the most restrictive set of privileges needed for the performance of authorized tasks.

Guidance

The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Applicability: All	**References:** ARS: AC-6; FISCAM: TSD-2.1; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); HSPD 7: D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2; NIST 800-53/53A: AC-6; PISP: 4.1.6	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6.1

Assessment Objective

Determine if:
(i) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks; and
(ii) the information system enforces the most restrictive set of rights/privileges or accesses needed by users.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.

AC-6(CMS-1) – Enhancement (High)		
Control Disable all file system access not explicitly required for system, application, and administrator functionality.		
Applicability: All	**References:** ARS: AC-6(CMS-1); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-6(CMS-1).1		
Assessment Objective Determine if the information system enforces separation of duties through assigned access authorizations. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if all file system access not explicitly required for system, application, and administrator functionality is disabled. **Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine hosts that store, transmit or process sensitive data to determine if file system access not explicitly required for system, application, and administrator functionality are disabled. **Test:** Information system hosts that store, transmit or process sensitive data to ensure that all file system access not explicitly required for system, application, and administrator functionality is disabled.		
AC-6(CMS-2) – Enhancement (High)		
Control Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.		
Applicability: All; Optional for SS	**References:** ARS: AC-6(CMS-2); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-6(CMS-2).1		
Assessment Objective Determine if the information system enforces separation of duties through assigned access authorizations. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if contractors are required to be provided with minimal system and physical access, and that they've agreed to support the CMS security requirements. The documented contractor selection process must assess the contractor's ability to adhere to and support CMS security policy. **Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine the default access levels given to contractors. Ensure that all file system access not explicitly required for system, application, and administrator functionality is disabled. **Test:** Information system hosts that store, transmit or process sensitive data; and that contain account information for contractors, to determine if all file system access not explicitly required for system, application, and administrator functionality is disabled.		
AC-6(CMS-3) – Enhancement (High)		
Control Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value levels. Implement column-level access controls.		
Applicability: All	**References:** ARS: AC-6(CMS-3); FISCAM: TAC-3.2.D.1, TAC-3.2.D.2, TAC-3.2.D.3, TAC-3.2.D.4	**Related Controls:**
ASSESSMENT PROCEDURE: AC-6(CMS-3).1		
Assessment Objective Determine if the information system enforces separation of duties through assigned access authorizations. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system restricts the use of database management utilities to only authorized database administrators. Policies and procedures must also prevent users from accessing database data files at the logical data view, field, or field-value levels. Implement column-level access controls. **Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine if the information system restricts the use of database management utilities to only authorized database administrators. Also, determine whether or not users are prevented from accessing database data files at the logical data view, field, or field-value levels. Column-level access controls must also be implemented. **Test:** Information system hosting databases to determine if the information system restricts the use of database management utilities to only authorized database administrators. Also, determine		

whether or not users are prevented from accessing database data files at the logical data view, field, or field-value levels. Column-level access controls must also be implemented.

AC-6(CMS-4) – Enhancement (High)

Control

Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.

Applicability: All	**References:** ARS: AC-6(CMS-4); FISCAM: TAN-2.2.1; HIPAA: 164.312(c)(1); HSPD 7: D(10); IRS-1075: 5.1#1.1, 5.2#1, 5.2#2, 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6(CMS-4).1

Assessment Objective

Determine if the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine if the default level of access for the various user types. Ensure that only access to those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties are assigned.

Test: Information system using a sample of user accounts with limited access, attempt to access files, directories, drives, workstations, servers, network shares, ports, protocols, or services that this user or user type has no access to.

AC-7 – Unsuccessful Log-on Attempts (High)

Control

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce a limit of CMS-defined consecutive invalid access attempts by a user during a specified time period. Systems shall be locked after a specified number of multiple unsuccessful log-on attempts.

Guidance

Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Applicability: All	**References:** ARS: AC-7; IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7	**Related Controls:**

ASSESSMENT PROCEDURE: AC-7.1

Assessment Objective

Determine if:

(i) the organization defines the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur;

(ii) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period;

(iii) the organization defines the time period for lock out mode or delay period;

(iv) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; and

(v) the information system enforces the organization-selected lock out mode or delayed login prompt.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing unsuccessful logon attempts; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts.

AC-7(0) – Enhancement (High)

Control

Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user during a one (1) hour time period. Require the lock out to persist for a minimum of three (3) hours.

Applicability: All	**References:** ARS: AC-7(0); IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7	**Related Controls:** AC-9

ASSESSMENT PROCEDURE: AC-7(0).1

Assessment Objective

Determine if the organization configures system lockout to assist in preventing password guessing.

Assessment Methods And Objects

Examine: Password lockout policy includes failed log-on attempts, lockout timeframes period for failed attempts and system/network administrator account reset capabilities.
Interview: A sampling of users for knowledge of log-on and account lockout procedure policy is known.
Test: The account lockout function requires and administrator's reset of the locked-out user account.

AC-8 – System Use Notification (High)

Control

An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS information system.

Guidance

Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Applicability: All	**References:** ARS: AC-8; FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2; NIST 800-53/53A: AC-8; PISP: 4.1.8	**Related Controls:** SI-4

ASSESSMENT PROCEDURE: AC-8.1

Assessment Objective

Determine if:
(i) the information system displays a system use notification message before granting system access informing potential users:
- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording;
(ii) the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).
(iii) the organization approves the information system use notification message before its use; and
(iv) the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for system use notification.

AC-8(CMS-1) – Enhancement (High)

Control

Configure the information system to display a warning banner automatically prior to granting access to potential users. Notify users that:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.

Guidance

All CMS information system computers and network devices under their control, independently, prominently and completely display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web, ftp, telnet, or other services accessed.

Applicability: All	**References:** ARS: AC-8(CMS-1); FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-1).1

Assessment Objective

Determine if the information system displays a system use notification message before granting system access informing potential users:
- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if the information system is configured to display a warning banner automatically prior to granting access to potential users. Notify users that:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.

Interview: Organizational personnel to determine if hosts are configured to present a warning banner at system access points. The warning banner must contain the following elements:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.

Test: Automated mechanisms implementing the access control policy for system use notification.

AC-8(CMS-2) – Enhancement (High)

Control

Develop and implement the warning banner in conjunction with legal counsel.

Applicability: All	**References:** ARS: AC-8(CMS-2); IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-2).1

Assessment Objective

Determine if the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if warning banners were developed and implemented in conjunction with legal counsel.

Interview: Organizational personnel to determine if warning banners were developed and implemented in conjunction with legal counsel.

Test: Automated mechanisms implementing the access control policy for system use notification.

AC-8(CMS-3) – Enhancement (High)

Control

Post clear privacy policies on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.

Applicability: All	**References:** ARS: AC-8(CMS-3); IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-3).1

Assessment Objective

Determine if the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if clear privacy policies are posted on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.

Interview: Organizational personnel to determine if clear privacy policies are posted where substantial personal information from the public is collected.

Test: Automated mechanisms implementing the access control policy for system use notification.

AC-9 – Previous Log-on Notification (High)

Control

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to provide users with information about previous log-ons, both successful and unsuccessful.

Guidance

Due to the possibility that an unauthorized person may have the ability to log-on to a system or application using an authorized person's log-on account, all systems and applicable applications will provide an automated method of notifying the authorized user of the last successful log-on date and time, and a number of previously unsuccessful log-on attempts. It is important that training include reporting procedures and responsibility for authorized users to report unauthorized log-ons and unauthorized attempts to log-on.

Applicability: All	References: ARS: AC-9; NIST 800-53/53A: AC-9; PISP: 4.1.9	Related Controls: AC-7(0), CA-4(1), CA-7(1)

ASSESSMENT PROCEDURE: AC-9.1

Assessment Objective

Determine if the information system, upon successful logon, displays the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing previous logon notification; information system notification messages; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing the access control policy for previous logon notification.(Optional)

AC-9(0) – Enhancement (High)

Control

Configure the information system to notify the user, upon successful log-on, of the date and time of the last log-on, and the number of unsuccessful log-on attempts since the last successful log-on.

Applicability: All	References: ARS: AC-9(0), 4.1.9	Related Controls:

ASSESSMENT PROCEDURE: AC-9(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing previous logon notification; information system notification messages; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for previous logon notification.

AC-10 – Concurrent Session Control (High)

Control

Automated mechanisms shall be in place to limit the number of concurrent user sessions, based upon the established business needs of the user, CMS, and the sensitivity level of the CMS information system.

Guidance

Some systems may require concurrent user sessions to function properly. However, based on the operational needs, automated mechanisms limit the number of concurrent user sessions. It is good practice to have management's approval for any system to have user concurrent sessions. Management should periodically review the need for user concurrent sessions.

Applicability: All	References: ARS: AC-10; NIST 800-53/53A: AC-10; PISP: 4.1.10	Related Controls:

ASSESSMENT PROCEDURE: AC-10.1

Assessment Objective

Determine if:

(i) the organization defines the maximum number of concurrent sessions for information system users; and

(ii) the information system limits the number of concurrent sessions for users to the organization-defined number of sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for concurrent session control.

AC-10(0) – Enhancement (High)		
Control The number of concurrent User ID network log-on sessions is limited and enforced to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties.		
Applicability: All	**References:** ARS: AC-10(0); NIST 800-53/53A: AC-10; PISP: 4.1.10	**Related Controls:**
ASSESSMENT PROCEDURE: AC-10(0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan (for organization-defined limit for concurrent sessions for information system users); other relevant documents or records. **Test:** Automated mechanisms implementing the access control policy for concurrent session control.		
AC-10(CMS-1) – Enhancement (High)		
Control The requirement and use of more than one (1) application/process session for each user is documented in the SSP.		
Applicability: All	**References:** ARS: AC-10(CMS-1)	**Related Controls:**
ASSESSMENT PROCEDURE: AC-10(CMS-1).1		
Assessment Objective Determine if the information system limits the number of concurrent sessions for users to the organization-defined number of sessions. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan (for organization-defined limit for concurrent sessions for information system users); other relevant documents or records to determine if the requirement and use of more than one (1) User ID network log-on session for each user is documented in the system risk assessment. **Interview:** Organizational personnel to determine if the information system allows more than one log-on session. **Test:** Automated mechanisms implementing the access control policy for concurrent session control.		
AC-11 – Session Lock (High)		
Control Automated session lock mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable locking of the information system session by the user. The information system shall also detect inactivity and block further access until the user re-establishes the connection using proper identification and authentication processes.		
Guidance Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.		
Applicability: All	**References:** ARS: AC-11; IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-11; PISP: 4.1.11	**Related Controls:**
ASSESSMENT PROCEDURE: AC-11.1		
Assessment Objective Determine if: (i) the organization defines the time period of user inactivity that initiates a session lock within the information system; (ii) the information system initiates a session lock after the organization-defined time period of inactivity; and (iii) the information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; information system security plan; other relevant documents or records. **Test:** Automated mechanisms implementing the access control policy for session lock.		
AC-11(0) – Enhancement (High)		
Control Configure systems to disable local access automatically after fifteen (15) minutes of inactivity. Require a password (see IA-5, Authenticator Management) to restore local access.		

Applicability: All	**References:** ARS: AC-11(0); FISCAM: TAC-3.2.C.3; IRS-1075: 5.6.3.2#4.3, 5.7.3#1; NIST 800-53/53A: AC-11; PISP: 4.1.11	**Related Controls:** IA-5

ASSESSMENT PROCEDURE: AC-11(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; information system security plan (for organization-defined time period for user inactivity after which automatic session lock is to be activated); other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for session lock.

AC-12 – Session Termination (High)

Control

The information system shall identify and terminate all inactive remote sessions (both user and information system sessions) automatically.

Guidance

A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Applicability: All	**References:** ARS: AC-12; FISCAM: TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-12; PISP: 4.1.12	**Related Controls:**

ASSESSMENT PROCEDURE: AC-12.1

Assessment Objective

Determine if:

(i) the organization defines the time period of user inactivity that initiates a remote session termination within the information system; and

(ii) the information system automatically terminates a remote session after the organization-defined time period of inactivity.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for session termination.

AC-12(0) – Enhancement (High)

Control

Configure the information system to automatically terminate all remote sessions (user and information system) after 30 minutes of inactivity.

Applicability: All	**References:** ARS: AC-12(0); FISCAM: TAC-3.2.C.3, TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-12; PISP: 4.1.12	**Related Controls:**

ASSESSMENT PROCEDURE: AC-12(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; information system security plan (for organization-defined time period for user inactivity after which automatic session termination is to be activated); other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for session termination.

AC-12(1) – Enhancement (High)

Control

Automatic session termination applies to local and remote sessions.

Applicability: All	**References:** ARS: AC-12(1); FISCAM: TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-12(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-12(1).1

Assessment Objective

Determine if automatic session termination applies to local and remote sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for session termination.

AC-13 – Supervision and Review—Access Control (High)

Control

Personnel shall be supervised and reviewed with respect to the usage of CMS information system access controls. Automated mechanisms shall be in place to facilitate the review of audit records, and any unusual activities shall be investigated in a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of users with significant information system roles and responsibilities shall be reviewed more frequently.

Guidance

The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**References:** ARS: AC-13; FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSD-3.2.1, TSD-3.2.3, TSS-2.1.3; HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: AC-13; PISP: 4.1.13	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13.1

Assessment Objective

Determine if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records.

Interview: Organizational personnel with supervisory and access control responsibilities.

AC-13(1) – Enhancement (High)

Control

Employ automated mechanisms to facilitate the review of user activities.

Applicability: All	**References:** ARS: AC-13(1); NIST 800-53/53A: AC-13(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(1).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.

AC-13(CMS-1) – Enhancement (High)

Control

Review integrity of files and directories for unexpected and/or unauthorized changes at least once per day. Automate the review of file creation, changes and deletions; and monitor permission changes. Generate alert notification for technical staff review and assessment.

Applicability: All	**References:** ARS: AC-13(CMS-1); FISCAM: TAC-2.1.5; HIPAA: 164.312(c)(2), 164.312(e)(2)(i)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(CMS-1).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records to determine if files and directories are reviewed for unexpected and/or unauthorized changes at least once per day. The review of file creation, changes and deletions, and permission changes must be monitored automatically. Alert notifications must be generated for technical staff review and assessment.

Interview: Organizational personnel with supervisory and access control responsibilities to determine if the integrity of files and directories for unexpected and/or unauthorized changes at least once per day. Determine if file creation, changes and deletions, and permission changes are being reviewed automatically. Determine if alert notifications for technical staff review and assessment are being generated.
Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.

AC-13(CMS-2) – Enhancement (High)

Control

Enable logging of administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations.

Applicability: All	**References:** ARS: AC-13(CMS-2); FISCAM: TAC-2.1.5, TAN-2.1.8, TSS-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(CMS-2).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records to determine if logging of administrator and user account activities, system shutdowns, reboots, errors and access authorizations is enabled.
Interview: Organizational personnel with supervisory and access control responsibilities to determine if logging of administrator and user account activities, system shutdowns, reboots, errors and access authorizations is enabled.
Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.

AC-13(CMS-3) – Enhancement (High)

Control

Inspect administrator groups, root accounts and other system related accounts on demand but at least once every seven (7) days to ensure that unauthorized accounts have not been created.

Applicability: All	**References:** ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(CMS-3).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system related accounts are inspected on demand, but at least once every seven (7) days to ensure that unauthorized accounts have not been created.
Interview: Organizational personnel with supervisory and access control responsibilities to determine if administrator groups, root accounts and other system related accounts are inspected on demand, but at least once every seven (7) days to ensure that unauthorized accounts have not been created.
Test: Automated mechanisms supporting the access control policy for supervision and review of user.

AC-13(FIS-1) – Enhancement (High)

Control

Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

Applicability: All	**References:** FISCAM: TSD-1.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(FIS-1).1

Assessment Objective

Determine if the organizational supervisory personnel review transactions performed.

Assessment Methods And Objects

Examine: Activities and test transaction reviews.
Examine: Pertinent policies and procedures.
Interview: Management.

AC-14 – Permitted Actions without Identification or Authentication (High)

Control

Based upon mission / business requirements, public access to CMS information systems without identification and authorization shall be limited to public websites and other publicly available

systems. CMS information systems shall be configured to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

Guidance

The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov).

Applicability: All	**References:** ARS: AC-14; NIST 800-53/53A: AC-14; PISP: 4.1.14	**Related Controls:** IA-2

ASSESSMENT PROCEDURE: AC-14.1

Assessment Objective

Determine if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for permitted actions without identification and authentication.

AC-14(0) – Enhancement (High)

Control

Identify and document specific user actions that can be performed on the information system without identification or authentication.

Applicability: All	**References:** ARS: AC-14(0); NIST 800-53/53A: AC-14; PISP: 4.1.14	**Related Controls:**

ASSESSMENT PROCEDURE: AC-14(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for permitted actions without identification and authentication.

AC-14(1) – Enhancement (High)

Control

Ensure that public users (users who have not been authenticated) only have access to the extent necessary to accomplish mission objectives while preventing unauthorized access to sensitive information.

Applicability: All	**References:** ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-14(1).1

Assessment Objective

Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; list of organization-defined actions that can be performed without identification and authentication; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining permitted actions without identification and authentication.

AC-15 – Automated Marking (High)

Control

Automated mechanisms shall be in place to mark CMS information system output using standard naming convention, in order to identify any special dissemination, handling, or distribution instructions.

Guidance

Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used for external marking are distinguished from the labels used on internal data structures described in AC-16.

Applicability: All	**References:** ARS: AC-15; NIST 800-53/53A: AC-15; PISP: 4.1.15	**Related Controls:** AC-16

ASSESSMENT PROCEDURE: AC-15.1

Assessment Objective

Determine if:
(i) the organization identifies standard naming conventions for information system output; and
(ii) the information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Assessment Methods And Objects

Examine: Access control policy; procedures for addressing automated marking of information system output; information system output; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel with responsibilities for defining special dissemination, handling, and marking instructions for information system output.
Test: Automated mechanisms implementing automated marking of information system output.

AC-16 – Automated Labeling (High)

Control

CMS information systems shall label information "in storage," "in process," and "in transit" with special dissemination handling or distribution instructions, in a manner consistent with this policy.

Guidance

Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.

Applicability: All	**References:** ARS: AC-16; NIST 800-53/53A: AC-16; PISP: 4.1.16	**Related Controls:** AC-15

ASSESSMENT PROCEDURE: AC-16.1

Assessment Objective

Determine if the information system appropriately labels information in storage, in process, and in transmission.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Automated mechanisms implementing automated (internal) labeling within the information system.(Optional)

AC-16(CMS-1) – Enhancement (High)

Control

If automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

Applicability: All	**References:** ARS: AC-16(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-16(CMS-1).1

Assessment Objective

Determine if the information system appropriately labels information in storage, in process, and in transmission.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine, if automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).
Interview: Organization personnel to determine, if automated information labeling is utilized, that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).
Test: Automated mechanisms implementing automated (internal) labeling within the information system.

AC-17 – Remote Access (High)

Control

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can access the information system from remote locations shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, shall not be used to gain access to a CMS information system that processes CMS sensitive information unless the CIO or his/her designated representative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-

up capabilities.

Guidance

Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST SP 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 and 800-78. NIST SP 800-77 provides guidance on IPSec-based virtual private networks.

Applicability: All	**References:** ARS: AC-17; FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17; PISP: 4.1.17	**Related Controls:** IA-2, SC-9

ASSESSMENT PROCEDURE: AC-17.1

Assessment Objective

Determine if the organization documents, monitors, and controls all methods of remote access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities.

AC-17(1) – Enhancement (High)

Control

Employ automated mechanisms to facilitate the monitoring and control of remote access methods.

Applicability: All	**References:** ARS: AC-17(1); IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(1).1

Assessment Objective

Determine if the information system employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for remote access.

AC-17(2) – Enhancement (High)

Control

Employ cryptography to protect the confidentiality and integrity of remote access sessions.

Applicability: All	**References:** ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(2).1

Assessment Objective

Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing cryptographic protections for remote access.

AC-17(3) – Enhancement (High)

Control

Control all remote access through a limited number of managed access control points.

Applicability: All	**References:** ARS: AC-17(3); IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(3)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(3).1

Assessment Objective

Determine if:

(i) the organization defines managed access control points for remote access to the information system; and
(ii) the information system controls all remote accesses through a limited number of managed access control points.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for remote access.

AC-17(4) – Enhancement (High)

Control

Permit remote access for privileged functions only for compelling operational needs and document the rationale for such access in the security plan for the information system.

Applicability: All	**References:** ARS: AC-17(4); FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(4)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(4).1

Assessment Objective

Determine if:
(i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed; and
(ii) the organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for remote access.

AC-17(CMS-1) – Enhancement (High)

Control

Enable secure management protocols through a VPN link(s) if connected to the information system and using remote administration. Utilize an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based).

Applicability: All	**References:** ARS: AC-17(CMS-1); IRS-1075: 5.6.3.2#5	**Related Controls:** SC-13

ASSESSMENT PROCEDURE: AC-17(CMS-1).1

Assessment Objective

Determine if the organization documents, monitors, and controls all methods of remote access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if secure management protocols through a VPN link(s) if connected to the information system and using remote administration are enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system.
Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if secure management protocols through a VPN link(s) if connected to the information system and using remote administration are enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system.
Test: Automated mechanisms implementing the access control policy for remote access to determine that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system.

AC-17(CMS-2) – Enhancement (High)

Control

Implement password protection for remote access connections.

Applicability: All	**References:** ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(CMS-2).1

Assessment Objective

Determine if the organization documents, monitors, and controls all methods of remote access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated

documentation; information system audit records; other relevant documents or records to determine if password protection for remote access connections is implemented.
Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if password protection is required for remote access connections.
Test: Automated mechanisms implementing the access control policy for remote access to determine remote access connections by attempting to gain access without a password.

AC-17(CMS-3) – Enhancement (High)

Control

Require callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified every 365 days.

Applicability: All	**References:** ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(CMS-3).1

Assessment Objective

Determine if:
(i) the organization defines managed access control points for remote access to the information system; and
(ii) the information system controls all remote accesses through a limited number of managed access control points.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified annually.
Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually.
Test: Automated mechanisms implementing the access control policy for remote access to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually.

AC-17(CMS-4) – Enhancement (High)

Control

If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix A for e-Authentication standards.

Applicability: All	**References:** ARS: AC-17(CMS-4); IRS-1075: 5.6.3.2#5	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(CMS-4).1

Assessment Objective

Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if e-authentication is implemented as a remote access solution or associated with remote access. If so, refer to ARS Appendix A for e-Authentication standards.
Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system implements e-authentication. If so, refer to ARS Appendix A for e-Authentication standards.
Test: Automated mechanisms implementing the access control policy for remote access to determine if e-authentication is implemented. If so, refer to ARS Appendix A for e-Authentication standards.

AC-17(FIS-1) – Enhancement (High)

Control

Remote access phone numbers are not published and are periodically changed.

Applicability: All	**References:** FISCAM: TAC-3.2.E.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(FIS-1).1

Assessment Objective

Determine if the organization changes, periodically, remote access phone numbers and those phone numbers are not published.

Assessment Methods And Objects

Examine: Documentation showing changes to dial-in numbers.
Examine: Entity's telephone directory to verify that the numbers are not listed.
Examine: Pertinent policies and procedures.
Interview: Remote access users.

AC-18 – Wireless Access Restrictions (High)

Control

Installation of wireless access points (WAP) into CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. Authorized WAP devices and wireless access shall be monitored on a regular basis, and wireless communications shall be secured through the use of approved encryption controls.

Guidance

NIST SP 800-48 and 800-97 provide guidance on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion detection and prevention.

Applicability: All	**References:** ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18	**Related Controls:**

ASSESSMENT PROCEDURE: AC-18.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for wireless technologies;
(ii) the organization authorizes, monitors, and controls wireless access to the information system; and
(iii) the wireless access restrictions are consistent with NIST SP 800-48 and 800-97.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records.
Test: Wireless access usage and restrictions.

AC-18(0) – Enhancement (High)

Control

CMS policy prohibits the use of wireless access unless explicitly approved by the CMS CIO or his/her designated representative.

Applicability: All	**References:** ARS: AC-18(0); NIST 800-53/53A: AC-18; PISP: 4.1.18	**Related Controls:**

ASSESSMENT PROCEDURE: AC-18(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records.
Test: Wireless access usage and restrictions.

AC-18(1) – Enhancement (High)

Control

If wireless access is explicitly approved, approved authentication and encryption is used to protect wireless access to the information system.

Applicability: All	**References:** ARS: AC-18(1); NIST 800-53/53A: AC-18(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-18(1).1

Assessment Objective

Determine if the organization uses authentication and encryption to protect wireless access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for wireless access to the information system.

AC-18(2) – Enhancement (High)		
Control Perform quarterly scans for unauthorized wireless access points and take appropriate action if any access points are discovered.		
Guidance Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.		
Applicability: All	**References:** ARS: AC-18(2); NIST 800-53/53A: AC-18(2)	**Related Controls:**
ASSESSMENT PROCEDURE: AC-18(2).1		
Assessment Objective Determine if: (i) the organization defines the frequency of scans for unauthorized wireless access points; and (ii) the organization scans for unauthorized wireless access points in accordance with organization-defined frequency and takes appropriate action if such an access points are discovered.		
Assessment Methods And Objects **Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records. **Test:** Scanning procedure for unauthorized wireless access points.		
AC-18(DIR-1) – Enhancement (High)		
Control If wireless access is explicitly approved, wireless devices, service set identifier broadcasting is disabled and the following wireless access controls are implemented: (a) encryption protection is enabled; (b) access points are placed in secure areas; (c) access points are shut down when not in use (i.e., nights, weekends); (d) a firewall is implemented between the wireless network and the wired infrastructure; (e) MAC address authentication is utilized; (f) static IP addresses, not DHCP, is utilized; (g) personal firewalls are utilized on all wireless clients; (h) file sharing is disabled on all wireless clients; (i) Intrusion detection agents are deployed on the wireless side of the firewall; and (j) wireless activity is monitored and recorded, and the records are reviewed on a regular basis.		
Applicability: All	**References:**	**Related Controls:**
ASSESSMENT PROCEDURE: AC-18(DIR-1).1		
Assessment Objective Determine if the organization establishes wireless policies and strict procedures that control access to the wireless LAN and separates/restricts the wireless LAN from the wired network infrastructure.		
Assessment Methods And Objects **Examine:** Access control procedures for continuous wireless intrusion monitoring of approved and operational wireless systems. **Interview:** Staff personnel who review the wireless LAN records know what to look for in the data for an unauthorized intrusion, and the staff knows the reporting procedures when an unauthorized intrusion is detected. **Test:** The wireless LAN does not allow rogue wireless devices into the approved wireless network infrastructure.		
AC-19 – Access Control for Portable and Mobile Devices (High)		
Control The connection of portable and mobile devices (e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CIO or his/her designated representative. Prior to connecting portable and mobile devices to CMS information systems and networks, such devices shall be configured to comply with CMS IS policies and procedures. The storage and transmission of CMS sensitive information on portable and mobile information devices shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware. The activities and controls shall be commensurate with the system security level of the information.		
Guidance Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management,		

scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family.

Applicability: All	**References:** ARS: AC-19; IRS-1075: 4.6#1; NIST 800-53/53A: AC-19; PISP: 4.1.19	**Related Controls:** MP-4, MP-5

ASSESSMENT PROCEDURE: AC-19.1

Assessment Objective

Determine if:
(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;
(ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and
(iii) the organization authorizes, monitors, and controls device access to organizational information systems.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Interview: Organizational personnel who use portable and mobile devices to access the information system.
Test: Automated mechanisms implementing access control policy for portable and mobile devices.

AC-19(CMS-1) – Enhancement (High)

Control

If portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative:
Employ an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Applicability: All	**References:** ARS: AC-19(CMS-1); FISCAM: TAC-3.3; IRS-1075: 4.6#1, 4.7.2#1	**Related Controls:** MA-CMS-1, MA-CMS-2, SC-13

ASSESSMENT PROCEDURE: AC-19(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;
(ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and
(iii) the organization authorizes, monitors, and controls device access to organizational information systems.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records to determine if portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative. Also, determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.
Interview: Organizational personnel who use portable and mobile devices to access the information system to determine if portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative. Also, determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.
Test: Automated mechanisms implementing access control policy for portable and mobile devices to determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

AC-20 – Use of External Information Systems (High)

Control

External information systems, including, but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports shall not be used to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative.

Strict terms and conditions shall be established for the use of external information systems. The terms and conditions shall address, at a minimum:
4.1.20.1. The types of applications that can be accessed from external information systems;

4.1.20.2. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
4.1.20.3. How other users of the external information system will be prevented from accessing federal information;
4.1.20.4. The use of virtual private networking (VPN) and firewall technologies;
4.1.20.5. The use of and protection against the vulnerabilities of wireless technologies;
4.1.20.6. The maintenance of adequate physical security controls;
4.1.20.7. The use of virus and spyware protection software; and
4.1.20.8. How often the security capabilities of installed software are to be updated.

Guidance

External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.
Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Applicability: All	**References:** ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20	**Related Controls:**

ASSESSMENT PROCEDURE: AC-20.1

Assessment Objective

Determine if:
(i) the organization defines the types of applications that can be accessed from the external information system;
(ii) the organization defines the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system; and
(iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel who use external information systems to access the information system.

AC-20(1) – Enhancement (High)

Control

Users are prohibited from using any external information system to access the information system or to process, store, or transmit CMS-controlled information except in situations where the organization:
(a) Can verify the employment of required security controls on the external system as specified in CMS' information security policy and the organization's system security plan; or
(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

Applicability: All	**References:** ARS: AC-20(1); IRS-1075: 4.7.2#1; NIST 800-53/53A: AC-20(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-20(1).1

Assessment Objective

Determine if the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:
- verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization's information security policy and system security plan when allowing connections to the external information system; or
- approves, for authorized exceptions, information system connection or processing agreements with the organizational entity hosting the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; information system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records.

AC-20(CMS-1) – Enhancement (High)

Control

Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.

Applicability: All	**References:** ARS: AC-20(CMS-1); IRS-1075: 4.7.2#1, 4.7.3#3	**Related Controls:**

ASSESSMENT PROCEDURE: AC-20(CMS-1).1

Assessment Objective

Determine if the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

Interview: Organizational personnel who use external information systems to access the information system to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

AC-20(PII-1) – Enhancement (High)

Control

Only organization owned computers and software can be used to process, access, and store PII.

Applicability: All	**References:** IRS-1075: 4.7.1#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-20(PII-1).1

Assessment Objective

Determine if the organizational computers and software are owned by that organization that processes, accesses and stores PII.

Assessment Methods And Objects

Examine: Organizational computer and software purchase orders indicating ownership of computers and software used to process, access and store PII.

Interview: Organizational staff indicating that only organizational owned computers and software are used to process, access and store PII.

AC-CMS-1 – System Boot Access (High)

Control

System boot access shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can alter or perform non-standard boots of systems and/or components of the information system shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Guidance

When a person has unrestrained physical access to any computing system or network device the person has control of the equipment.
If the person does not have the capability to locally access the information system's data though the boot process this can assist in protecting the data from loss or unauthorized access to the data.
Note: Even though the system root access may be protected by privilege access controls a miss configured system can allow the system to reboot and thus allowing a boot / access from unauthorized media. An example of this is a LINUX system, not configured correctly, when CONT+ALT+DEL is issued from the keyboard the equipment will re-boot automatically.

Applicability: All	**References:** ARS: AC-CMS-1; PISP: 4.1.21	**Related Controls:**

ASSESSMENT PROCEDURE: AC-CMS-1.1

Assessment Objective

Determine if the organization assesses the need for system boot access and if necessary controls, documents and monitors the continued need for system boot access.

Assessment Methods And Objects

Examine: System boot access documentation to determine that there is or is not a need for boot access.

Interview: Organizational personnel to determine that there is or is not a need for system boot access.

AC-CMS-1(CMS-1) – Enhancement (High)		
Control If not explicitly required, boot access to removable media drives is disabled.		
Applicability: All	**References:** ARS: AC-CMS-1(CMS-1)	**Related Controls:**
ASSESSMENT PROCEDURE: AC-CMS-1(CMS-1).1		
Assessment Objective Determine if the organization evaluates the need for system boot access by removable media drives. **Assessment Methods And Objects** **Examine:** System boot access documentation to determine that, if not explicitly required, boot access to removable media drives is disabled. **Interview:** Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled. **Test:** Information system sample of workstations to determine if boot access to removable media drives is disabled.		
AC-CMS-1(CMS-2) – Enhancement (High)		
Control System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).		
Applicability: All	**References:** ARS: AC-CMS-1(CMS-2)	**Related Controls:** IA-5
ASSESSMENT PROCEDURE: AC-CMS-1(CMS-2).1		
Assessment Objective Determine if the organization controls access to the system BIOS when unauthorized personnel may be in physical proximity to the system. **Assessment Methods And Objects** **Examine:** System BIOS documentation to determine if System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management). **Interview:** Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled. **Test:** Information system sample of workstations by attempting to access the System BIOS. Ensure that access to the System BIOS is protected by password.		
AC-CMS-1(CMS-3) – Enhancement (High)		
Control If not explicitly required, removable media drive functionality is disabled.		
Applicability: All	**References:** ARS: AC-CMS-1(CMS-3)	**Related Controls:**
ASSESSMENT PROCEDURE: AC-CMS-1(CMS-3).1		
Assessment Objective Determine if the organization disables removable media drive functionality If not explicitly required. **Assessment Methods And Objects** **Examine:** Removable media drive documentation to determine that, if not explicitly required, removable media drive functionality is disabled. **Interview:** Organizational personnel to determine that, if not explicitly required, removable media drive functionality is disabled. **Test:** Sample of Information system workstations to determine if removable media drive functionality is disabled.		

Awareness and Training (AT) – *Operational*

AT-1 – Security Awareness and Training Policy and Procedures (High)

Control

An IS AT program shall be developed, documented, and implemented effectively for all personnel, including contractors and any other users of CMS information and information systems. The IS AT program shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information, information systems, and networks.

Guidance

The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-16 and 800-50 provide guidance on security awareness and training. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AT-1; FISCAM: TSP-4.2.2; IRS-1075: 5.6.2.7#1.1-2, 6.1#1; NIST 800-53/53A: AT-1; PISP: 4.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AT-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security awareness and training policy and procedures;
(ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review security awareness and training policy and procedures; and
(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.
Interview: Organizational personnel with security awareness and training responsibilities.

ASSESSMENT PROCEDURE: AT-1.2

Assessment Objective

Determine if:
(i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.
Interview: Organizational personnel with security awareness and training responsibilities.

AT-2 – Security Awareness (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS AT program shall be consistent with 5 CFR Part 930 (http://opm.gov/fedregis/2004/69-061404-32835-a.pdf) and the guidance provided in NIST SP 800-50.

Guidance

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	**References:** ARS: AT-2; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3; NIST 800-53/53A: AT-2; PISP: 4.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2.1

Assessment Objective

Determine if:

(i) the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes;
(ii) the security awareness training is consistent with applicable regulations and NIST SP 800-50;
(iii) the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access;
(iv) the organization defines the frequency of refresher security awareness training; and
(v) the organization provides refresher security awareness training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan; other relevant documents or records.
Interview: Organizational personnel comprising the general information system user community.

AT-2(0) – Enhancement (High)

Control

All information system users (including managers and senior executives) receive basic information security awareness training prior to accessing any system's information; when required by system changes; and every 365 days thereafter.

Applicability: All	**References:** ARS: AT-2(0); FISCAM: TSP-3.3.1; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3, 6.2#1.1-2, 6.2#1.4, 6.2#2.1; NIST 800-53/53A: AT-2; PISP: 4.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan (for organization-defined frequency of refresher security awareness training); other relevant documents or records.
Interview: Organizational personnel comprising the general information system user community.

AT-2(CMS-1) – Enhancement (High)

Control

Establish a program to promote continuing awareness of information security issues and threats.

Applicability: All	**References:** ARS: AT-2(CMS-1); HIPAA: 164.308(a)(5)(ii)(A); IRS-1075: 5.6.2.7#1.3	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2(CMS-1).1

Assessment Objective

Determine if the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records to determine that a program to promote continuing awareness of information security issues and threats has been established.
Interview: Organizational personnel with security awareness and training responsibilities to determine that a program to promote continuing awareness of information security issues and threats has been established.

AT-3 – Security Training (High)

Control

The organization shall identify and document all positions and/or roles with significant information system security responsibilities during the system development life cycle. All personnel with significant information system security responsibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Content of the security awareness training shall be determined based upon the information systems to which personnel have authorized access. The employee shall acknowledge having received the security and awareness training either in writing or electronically as part of the training course completion.

Guidance

The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	References: ARS: AT-3; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	Related Controls:

ASSESSMENT PROCEDURE: AT-3.1

Assessment Objective

Determine if:
(i) the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities;
(ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes;
(iii) the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security;
(iv) the security training is consistent with applicable regulations and NIST SP 800-50;
(v) the organization defines the frequency of refresher security training; and
(vi) the organization provides refresher security training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan; other relevant documents or records.
Interview: Organizational personnel with significant information system security responsibilities.

AT-3(0) – Enhancement (High)

Control

Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to CMS networks, systems, and/or applications; when required by system changes; and refresher training every 365 days thereafter.

Applicability: All	References: ARS: AT-3(0); FISCAM: TSP-3.3.1; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	Related Controls:

ASSESSMENT PROCEDURE: AT-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan (for organization-defined frequency of refresher security training); other relevant documents or records.
Interview: Organizational personnel with significant information system security responsibilities.

AT-4 – Security Training Records (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that individual IS training activities, including basic security awareness training and specific information system security training, are properly documented and monitored.

Guidance

Procedures and training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.
(2) Executives must receive training in information security basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.

(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	**References:** ARS: AT-4; FISCAM: TSP-4.2.3; IRS-1075: 6.2#1.3; NIST 800-53/53A: AT-4; PISP: 4.2.4	**Related Controls:**

ASSESSMENT PROCEDURE: AT-4.1

Assessment Objective

Determine if the organization monitors and documents basic security awareness training and specific information system security training.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.

AT-5 – Contacts with Security Groups and Associations (High)

Control

Contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations shall be encouraged and supported to enable security personnel to stay up to date with the latest recommended security practices, techniques, and technologies; and to share the latest security-related information including threats, vulnerabilities, and incidents.

Guidance

To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Applicability: All	**References:** ARS: AT-5; HSPD 7: H(25); NIST 800-53/53A: AT-5; PISP: 4.2.5	**Related Controls:**

ASSESSMENT PROCEDURE: AT-5.1

Assessment Objective

Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security techniques and technologies and to share security-related information.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records.(Optional)

Audit and Accountability (AU) – *Technical*

AU-1 – Audit and Accountability Policy and Procedures (High)

Control

All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the implementation and management of audit controls, and shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AU-1; IRS-1075: 5.6.3.3#1; NIST 800-53/53A: AU-1; PISP: 4.3.1	**Related Controls:**

ASSESSMENT PROCEDURE: AU-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents audit and accountability policy and procedures;
(ii) the organization disseminates audit and accountability policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review audit and accountability policy and procedures; and
(iv) the organization updates audit and accountability policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Audit and accountability policy and procedures; other relevant documents or records.
Interview: Organizational personnel with audit and accountability responsibilities.

ASSESSMENT PROCEDURE: AU-1.2

Assessment Objective

Determine if:
(i) the audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Audit and accountability policy and procedures; other relevant documents or records.
Interview: Organizational personnel with audit and accountability responsibilities.

AU-2 – Auditable Events (High)

Control

Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security incidents. The selection of auditable events shall be based upon a risk assessment as to which events require auditing on a continuous basis, and which events require auditing in response to specific situations.

Guidance

The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**References:** ARS: AU-2; FISCAM: TAC-4.3.4, TSD-3.2.2; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2; PISP: 4.3.2	**Related Controls:** AU-4

ASSESSMENT PROCEDURE: AU-2.1

Assessment Objective

Determine if:
(i) the organization defines information system auditable events;
(ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and
(iii) the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing information system auditing of organization-defined auditable events.

AU-2(0) – Enhancement (High)

Control

Generate audit records for the following events:
(a) User account management activities,
(b) System shutdown,
(c) System reboot,
(d) System errors,
(e) Application shutdown,
(f) Application restart,
(g) Application errors,
(h) File creation,
(i) File deletion,
(j) File modification,
(k) Failed and successful log-ons,
(l) Security policy modifications,
(m) Use of administrator privileges, and
(n) File access.

Guidance

Note: For FTI, generate audit records for the following events in addition to those specified in other controls:
(a) All successful and unsuccessful authorization attempts.
(b) All changes to logical access control authorities (e.g., rights, permissions).
(c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
(d) The audit trail shall capture the enabling or disabling of audit report generation services.
(e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

Applicability: All	**References:** ARS: AU-2(0); FISCAM: TAC-2.1.5, TAC-4.1, TSD-3.2.4; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3; NIST 800-53/53A: AU-2; PISP: 4.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing information system auditing of organization-defined auditable events.

AU-2(1) – Enhancement (High)

Control

Provide the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical) time correlated audit trail.

Applicability: All	**References:** ARS: AU-2(1); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(1).1

Assessment Objective

Determine if:
(i) the organization defines the components of the information system that generate audit records; and
(ii) the information system compiles audit records from the organization-defined (multiple) components within the information system into a systemwide (logical or physical), time-correlated audit trail.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing a system-wide auditing capability.

AU-2(2) – Enhancement (High)

Control

Provide the capability to manage the selection of events to be audited by individual components of the information system.

Applicability: All	**References:** ARS: AU-2(2); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(2).1

Assessment Objective

Determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing Information system auditing for the specified components of the information system.

AU-2(3) – Enhancement (High)

Control

Periodically review and update the list of auditable events.

Applicability: All	**References:** ARS: AU-2(3); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2(3)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(3).1

Assessment Objective

Determine if the organization periodically reviews and updates the list of organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records.
Interview: Organizational personnel with auditing and accountability responsibilities.

AU-2(CMS-1) – Enhancement (High)

Control

Enable logging for perimeter devices, including firewalls and routers.
(a) Log packet screening denials originating from un-trusted networks,
(b) Packet screening denials originating from trusted networks,
(c) User account management,
(d) Modification of proxy services,
(e) Application errors,
(f) System shutdown and reboot,
(g) System errors,
(h) Modification of proxy services, and
(i) Modification of packet filters.

Applicability: All	**References:** ARS: AU-2(CMS-1); HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(CMS-1).1

Assessment Objective

Determine if:

(i) the organization defines information system auditable events;
(ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and
(iii) the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if logging-on is enabled for perimeter devices, including firewalls and routers. This logging will capture the following information:
(a) Log packet screening denials originating from un-trusted networks,
(b) packet screening denials originating from trusted networks,
(c) user account management,
(d) modification of proxy services,
(e) application errors,
(f) system shutdown and reboot,
(g) system errors,
(h) modification of proxy services, and
(i) modification of packet filters.

Interview: Organizational personnel with audit and accountability responsibilities to determine if logging-on is enabled for perimeter devices, including firewalls and routers. This logging will capture the following information:
(a) Log packet screening denials originating from un-trusted networks,
(b) packet screening denials originating from trusted networks,
(c) user account management,
(d) modification of proxy services,
(e) application errors,
(f) system shutdown and reboot,
(g) system errors,
(h) modification of proxy services, and
(i) modification of packet filters.

Test: Automated mechanisms implementing information system auditing of organization-defined auditable events.

AU-2(CMS-2) – Enhancement (High)

Control

Verify that proper logging is enabled in order to audit administrator activities.

Applicability: All	**References:** ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(CMS-2).1

Assessment Objective

Determine if the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if proper logging is enabled in order to audit administrator activities.

Interview: Organizational personnel with account audit and accountability responsibilities to determine if proper logging is enabled in order to audit administrator activities.

Test: Automated mechanisms implementing information system auditing of organization-defined auditable events.

AU-3 – Content of Audit Records (High)

Control

Automated mechanisms shall be established to provide the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome.

Guidance

Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**References:** ARS: AU-3; FISCAM: TAC-3.2.D.1, TAN-2.1.9; IRS-1075: 5.6.3.3#3; NIST 800-53/53A:	**Related Controls:**

	AU-3; PISP: 4.3.3	

ASSESSMENT PROCEDURE: AU-3.1

Assessment Objective

Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records.

Test: Automated mechanisms implementing information system auditing of auditable events.

AU-3(1) – Enhancement (High)

Control

Provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

Applicability: All	**References:** ARS: AU-3(1); NIST 800-53/53A: AU-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-3(1).1

Assessment Objective

Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject.

AU-3(2) – Enhancement (High)

Control

Centrally manage the content of audit records generated by individual components throughout the system.

Applicability: All	**References:** ARS: AU-3(2); NIST 800-53/53A: AU-3(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-3(2).1

Assessment Objective

Determine if the information system provides the capability to centrally manage the content of audit records generated from multiple components throughout the system.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system auditing with central management capability.

AU-3(CMS-1) – Enhancement (High)

Control

Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still required.

Applicability: All	**References:** ARS: AU-3(CMS-1); FISCAM: TAC-4.1; HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AU-3(CMS-1).1

Assessment Objective

Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing the content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records to determine if the organization records disclosures of sensitive information, including protected health and financial information. The organization must log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still required.

Interview: Organizational personnel with account audit and accountability responsibilities to determine if the organization records disclosures of sensitive information, including protected health and financial information. The organization must log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still required.

Test: Automated mechanisms implementing information system auditing of auditable events with organization-defined audit record content.

AU-4 – Audit Storage Capacity (High)

Control

A sufficient amount of information system storage capacity shall be allocated for audit records, and information systems shall be configured to reduce the likelihood of audit records exceeding such storage capacity.

Guidance

The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements.

Applicability: All	References: ARS: AU-4; IRS-1075: 5.6.3.3#4; NIST 800-53/53A: AU-4; PISP: 4.3.4	Related Controls: AU-2, AU-5, AU-6, AU-7, SI-4

ASSESSMENT PROCEDURE: AU-4.1

Assessment Objective

Determine if:
(i) the organization defines audit record storage capacity for the information system components that generate audit records; and
(ii) the organization establishes information system configuration settings to reduce the likelihood of the audit record storage capacity being exceeded.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components generating audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AU-5 – Response to Audit Processing Failures (High)

Control

Automated mechanisms shall be established which provide the capability to generate information system alerts for appropriate officials in the event of an audit failure or audit storage capacity being reached and to take appropriate additional actions.

Guidance

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Applicability: All	References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5	Related Controls: AU-4

ASSESSMENT PROCEDURE: AU-5.1

Assessment Objective

Determine if:
(i) the organization defines actions to be taken in the event of an audit processing failure;
(ii) the organization defines personnel to be notified in case of an audit processing failure; and
(iii) the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure or audit storage capacity being reached.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system response to audit processing failures.

AU-5(0) – Enhancement (High)

Control

Alert appropriate officials and take the following actions in response to an audit failure or audit storage capacity issue:
(a) Shutdown the information system,
(b) Stop generating audit records, or
(c) Overwrite the oldest records, in the case that storage media is unavailable.

Applicability: All	References: ARS: AU-5(0); NIST 800-53/53A: AU-5; PISP: 4.3.5	Related Controls:

ASSESSMENT PROCEDURE: AU-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for list of actions

to be taken by the information system in case of an audit processing failure); information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system response to audit processing failures.

AU-5(1) – Enhancement (High)

Control

The information system provides a warning when allocated audit record storage volume reaches 80% of audit record storage capacity.

Applicability: All	**References:** ARS: AU-5(1); NIST 800-53/53A: AU-5(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-5(1).1

Assessment Objective

Determine if:
(i) the organization defines percentage of maximum audit record storage capacity; and
(ii) the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing audit storage limit warnings.

AU-5(2) – Enhancement (High)

Control

A second real-time alert is sent when the audit record log is full.

Applicability: All	**References:** ARS: AU-5(2); NIST 800-53/53A: AU-5(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-5(2).1

Assessment Objective

Determine if:
(i) the organization defines audit failure events requiring real-time alerts; and
(ii) the information system provides a real-time alert when organization-defined audit failure events occur.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing real time audit alerts.

AU-6 – Audit Monitoring, Analysis, and Reporting (High)

Control

Information system audit records shall be reviewed and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and/or suspicious activity. Such activity shall be investigated and reported to appropriate officials, in accordance with current CMS Procedures.

Guidance

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Applicability: All	**References:** ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6	**Related Controls:** AU-4, IR-4

ASSESSMENT PROCEDURE: AU-6.1

Assessment Objective

Determine if:
(i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity;
(ii) the organization investigates suspicious activity or suspected violations;
(iii) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and
(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit

records; other relevant documents or records.
Test: Information system audit monitoring, analysis, and reporting capability.

ASSESSMENT PROCEDURE: AU-6.2

Assessment Objective

Determine if the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Interview: Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities.

AU-6(1) – Enhancement (High)

Control

Employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Applicability: All	**References:** ARS: AU-6(1); HIPAA: 164.312(b); NIST 800-53/53A: AU-6(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms integrating audit monitoring, analysis, and reporting into an organizational process for investigation and response to suspicious activities.

AU-6(2) – Enhancement (High)

Control

Employ automated mechanisms to immediately alert security personnel of the following minimal examples of inappropriate or unusual activities with security implications: threats to infrastructure, systems or assets; threats to CMS sensitive data; and threats to finances, personnel, or property.

Applicability: All	**References:** ARS: AU-6(2); HIPAA: 164.312(b); NIST 800-53/53A: AU-6(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(2).1

Assessment Objective

Determine if:
(i) the organization defines inappropriate or unusual activities with security implications; and
(ii) the organization employs automated mechanisms to alert security personnel of the occurrence of any organization-defined inappropriate or unusual activities with security implications.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing security alerts.

AU-6(CMS-1) – Enhancement (High)

Control

Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Applicability: All	**References:** ARS: AU-6(CMS-1); FISCAM: TAC-4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-1).1

Assessment Objective

Determine if:
(i) the organization regularly reviews / analyzes audit records for indications of inappropriate or unusual activity;
(ii) the organization investigates suspicious activity or suspected violations;
(iii) the organization reports findings of inappropriate/usual activities, suspicious behavior, or suspected violations to appropriate officials; and
(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Interview: Organizational personnel responsible for audit and accountability to determine if initialization sequences, log-ons and errors; system processes and performance; and system resource utilization are recorded to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Test: Information system audit monitoring, analysis, and reporting capability to determine if initialization sequences, log-ons and errors; system processes and performance; and system resource utilization are recorded to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

AU-6(CMS-2) – Enhancement (High)

Control

Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Applicability: All	**References:** ARS: AU-6(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-2).1

Assessment Objective

Determine if the organization regularly reviews / analyzes audit records for indications of inappropriate or unusual activity.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Interview: Organizational personnel responsible for audit and accountability to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Test: Information system audit monitoring, analysis, and reporting capability to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

AU-6(CMS-3) – Enhancement (High)

Control

Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.

Applicability: All	**References:** ARS: AU-6(CMS-3); FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.3, TAC-4.3.4; HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-3).1

Assessment Objective

Determine if the organization investigates suspicious activity or suspected violations.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.

Interview: Organizational personnel responsible for audit and accountability to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.

Test: Information system audit monitoring, analysis, and reporting capability to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.

AU-6(CMS-4) – Enhancement (High)

Control

Use automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

Applicability: All	**References:** ARS: AU-6(CMS-4); HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-4).1

Assessment Objective

Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

Interview: Organizational personnel responsible for audit and accountability to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

Test: Information system audit monitoring, analysis, and reporting capability to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

AU-6(CMS-5) – Enhancement (High)

Control

Inspect administrator groups on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Applicability: All	**References:** ARS: AU-6(CMS-5); FISCAM: TAC-2.1.5; HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-5).1

Assessment Objective

Determine if the organization monitors activities of system administrators.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Interview: Organizational personnel with audit and accountability responsibilities to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Test: Information system audit monitoring, analysis, and reporting capability to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

AU-6(CMS-6) – Enhancement (High)

Control

Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Applicability: All	**References:** ARS: AU-6(CMS-6); HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-6).1

Assessment Objective

Determine if the organization randomly performs a manual review of automated audit systems to validate the correctness of the automated system.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Interview: Organizational personnel with audit and accountability responsibilities to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Test: Information system audit monitoring, analysis, and reporting capability to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

AU-6(FIS-1) – Enhancement (High)

Control

The use of privileged system software and utilities is reviewed by technical management. Systems programmers' activities are monitored and reviewed. Inappropriate or unusual activity in using utilities is investigated.

Applicability: All	**References:** FISCAM: TSS-2.2.1, TSS-2.2.2, TSS-2.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(FIS-1).1

Assessment Objective

Determine if the organization monitors and reviews system programmers' activities and investigates inappropriate or unusual activities when using privileged system software utilities.

Assessment Methods And Objects

Examine: Documentation supporting the supervising and monitoring of systems programmers' activities.
Examine: Documentation supporting their reviews.
Examine: Documentation supporting these investigations.
Examine: Pertinent policies and procedures.
Interview: Systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
Interview: Technical management regarding their reviews of privileged system software and utilities usage.

AU-6(IRS-1) – Enhancement (High)

Control

For FTI, all requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log. (see IRS Pub. 1075, sect 6.3.1)

Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	**References:** IRS-1075: 6.3.1#1	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(IRS-1).1

Assessment Objective

Determine if the organization maintains a log for all requests for returned FTI, and the log includes receipt and/or disposal of returns (see IRS Pub. 1075, sect 6.3.1).

Assessment Methods And Objects

Examine: Logs for requests of FTI include receipt and/or disposal or FTI information is returned.
Interview: Responsible organizational staff handling FTI to determine is there is an effective log of FTI requests, disposal or returns.

AU-7 – Audit Reduction and Report Generation (High)

Control

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to enable human review of audit information and the generation of appropriate audit reports.

Guidance

Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Applicability: All	**References:** ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7	**Related Controls:** AU-4

ASSESSMENT PROCEDURE: AU-7.1

Assessment Objective

Determine if the information system provides an audit reduction and report generation capability.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records.
Interview: Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities.
Test: Audit reduction and report generation capability.

AU-7(1) – Enhancement (High)

Control

Employ a system capability that automatically processes audit records for events of interest based upon selectable, event criteria.

Applicability: All	**References:** ARS: AU-7(1); NIST 800-53/53A: AU-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-7(1).1

Assessment Objective

Determine if the information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records.
Test: Audit reduction and report generation capability.

AU-8 – Time Stamps (High)		
Control Audit records shall employ time stamps for use in audit record generation. Time stamps of audit records shall be generated using internal system clocks that are synchronized system-wide.		
Guidance Time stamps (including date and time) of audit records are generated using internal system clocks.		
Applicability: All	**References:** ARS: AU-8; NIST 800-53/53A: AU-8; PISP: 4.3.8	**Related Controls:**
ASSESSMENT PROCEDURE: AU-8.1		
Assessment Objective Determine if the information system provides time stamps for use in audit record generation. **Assessment Methods And Objects** **Examine:** Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test:** Automated mechanisms implementing time stamp generation.		
AU-8(1) – Enhancement (High)		
Control Information system clock synchronization occurs daily and at system boot.		
Applicability: All	**References:** ARS: AU-8(1); NIST 800-53/53A: AU-8(1)	**Related Controls:**
ASSESSMENT PROCEDURE: AU-8(1).1		
Assessment Objective Determine if: (i) the organization defines the frequency of internal clock synchronization for the information system; and (ii) the organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency. **Assessment Methods And Objects** **Examine:** Audit and accountability policy; procedures addressing time stamp generation; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test:** Automated mechanisms implementing internal information system clock synchronization.		
AU-9 – Protection of Audit Information (High)		
Control Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.		
Guidance Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.		
Applicability: All	**References:** ARS: AU-9; NIST 800-53/53A: AU-9; PISP: 4.3.9	**Related Controls:**
ASSESSMENT PROCEDURE: AU-9.1		
Assessment Objective Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion. **Assessment Methods And Objects** **Examine:** Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records. **Test:** Automated mechanisms implementing audit information protection.		
AU-9(1) – Enhancement (High)		
Control Employ automated mechanisms that are restricted to hardware-enforced, “write-once” media for recording audit information (e.g., CD-R, not CD-RW).		
Applicability: All	**References:** ARS: AU-9(1); NIST 800-53/53A: AU-9(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-9(1).1

Assessment Objective

Determine if the information system produces audit information on hardware-enforced, write-once media.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; other relevant documents or records.(Optional)

Test: Media storage devices.(Optional)

AU-10 – Non-Repudiation (High)

Control

Non-repudiation mechanisms shall be implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message.

Guidance

Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Applicability: All	**References:** ARS: AU-10; NIST 800-53/53A: AU-10; PISP: 4.3.10	**Related Controls:**

ASSESSMENT PROCEDURE: AU-10.1

Assessment Objective

Determine if the information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing non-repudiation capability.(Optional)

AU-11 – Audit Record Retention (High)

Control

Audit records shall be retained to provide support for after-the-fact investigations of security incidents, and to meet regulatory and/or CMS information retention requirements. The National Archives and Records Administration maintains criteria for record retention across many disciplines and information security retention standards shall not be construed to relieve or waive these other standards.

Guidance

The organization retains audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions (CMS sensitive information retention). Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST SP 800-61 provides guidance on computer security incident handling and audit record retention.

Applicability: All	**References:** NIST 800-53/53A: AU-11	**Related Controls:**

ASSESSMENT PROCEDURE: AU-11.1

Assessment Objective

Determine if:

(i) the organization defines the retention period for audit records generated by the information system; and

(ii) the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information system audit record retention responsibilities.

AU-11(0) – Enhancement (High)		
Control Retain audit records for ninety (90) days, and archive old audit records. Retain audit record archives for one (1) year.		
Applicability: All	**References:** ARS: AU-11(0); NIST 800-53/53A: AU-11; PISP: 4.3.11	**Related Controls:**
ASSESSMENT PROCEDURE: AU-11(0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information system audit record retention responsibilities.		
AU-11(PII-1) – Enhancement (High)		
Control Employ mechanisms to facilitate the review of PII disclosure/access records and retain the records for five (5) years or the applicable records control schedule, whichever is longer.		
Applicability: All	**References:** IRS-1075: 3.1#1	**Related Controls:**
ASSESSMENT PROCEDURE: AU-11(PII-1).1		
Assessment Objective Determine if the organization employs mechanisms to facilitate the review of PII disclosures/access records and retains the records for five (5) years or the applicable records control schedule, whichever is longer. **Assessment Methods And Objects** **Examine:** PII disclosure/access audit records are retained or a control schedule indicates (5) five years or longer.		
AU-11(PII-2) – Enhancement (High)		
Control To support the audit of activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever PII is stored.		
Applicability: All	**References:** IRS-1075: 5.6.3.3#5.2	**Related Controls:**
ASSESSMENT PROCEDURE: AU-11(PII-2).1		
Assessment Objective Determine if the organization ensures that audit information is archived for six (6) years to enable the recreation of computer related accesses to both the operation system and the application wherever PII is stored. **Assessment Methods And Objects** **Examine:** PII audit information is retained for (6) six years to enable recreation of computer related access to both the operation system and the application wherever PII is stored.		
AU-11(PII-3) – Enhancement (High)		
Control For PII, inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.		
Applicability: All	**References:** IRS-1075: 6.3.5#3	**Related Controls:**
ASSESSMENT PROCEDURE: AU-11(PII-3).1		
Assessment Objective Determine if the organizational PII inspection reports include a record of corrective actions, which is retained for a minimum of three (3) years from the date the inspection was completed. **Assessment Methods And Objects** **Examine:** PII inspection records to determine inclusion of corrective actions and are retained for a minimum of three (3) years from the inspection completion date.		

Certification, Accreditation, and Security Assessments (CA) – *Management*

CA-1 – Certification, Accreditation, and Security Assessments Policies and Procedures (High)

Control

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the Business Owner and accredited by the CMS CIO or his/her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the confidentiality, integrity, and availability (CIA) of CMS information and information systems. All C&A and security assessment activities shall be conducted in accordance with current CMS Procedures.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs, MAs, and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and/or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.4.6, Security Accreditation (CA-6).

If the CMS CIO or his/her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his/her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his/her designated representatives.

As part of the system certification and accreditation (C&A), an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, IS Risk Assessment (RA), System Security Plan (SSP), independent system tests and evaluations, the Business Owner and System Developer / Maintainer shall certify that the system meets the security requirements to the extent necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CMS CIO or the Designated Accrediting Authority (DAA).

Guidance

The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CA-1; FISCAM: TSP-5.1.2; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 5.6.1.4#1.1-2; NIST 800-53/53A: CA-1; PISP: 4.4.1	**Related Controls:** CA-6

ASSESSMENT PROCEDURE: CA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security assessment and certification and accreditation policies and procedures;
(ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review policy and procedures; and
(iv) the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.
Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.

ASSESSMENT PROCEDURE: CA-1.2

Assessment Objective

Determine if:
(i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.

Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.

CA-2 – Security Assessments (High)

Control

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application, and comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Routine assessments shall be conducted every 365 days, in accordance with NIST SP 800-53 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST SP 800-53 A provides guidance on security control assessments to include reuse of existing assessment results.

Applicability: All	**References:** ARS: CA-2; FISCAM: TSP-5.1.1; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1; NIST 800-53/53A: CA-2; PISP: 4.4.2	**Related Controls:** CA-4, CA-6, CA-7, CA-7(1), SA-11, SI-2

ASSESSMENT PROCEDURE: CA-2.1

Assessment Objective

Determine if:

(i) the information system is in the inventory of major information systems; and

(ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security assessment policy; procedures addressing security assessments; information system security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records.

CA-3 – Information System Connections (High)

Control

Management shall authorize in writing through the use of system connection agreements all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system connections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

Guidance

Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST SP 800-47 provides guidance on connecting information systems.

Applicability: All	**References:** ARS: CA-3; HSPD 7: F(19); NIST 800-53/53A: CA-3; PISP: 4.4.3	**Related Controls:** SA-9, SC-7

ASSESSMENT PROCEDURE: CA-3.1

Assessment Objective

Determine if:

(i) the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary);

(ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements;
(iii) the organization monitors/controls the system interconnections on an ongoing basis; and
(iv) information system connection agreements are consistent with NIST SP 800-47.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements.

CA-3(CMS-1) – Enhancement (High)

Control

Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

Applicability: All	**References:** ARS: CA-3(CMS-1); FISCAM: TAC-2.1.3; HSPD 7: F(19)	**Related Controls:**

ASSESSMENT PROCEDURE: CA-3(CMS-1).1

Assessment Objective

Determine if the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.
Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

CA-4 – Security Certification (High)

Control

Business owners shall conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification process shall be integrated into and span across the SDLC. In addition, the Business Owner shall review the certification documentation every 365 days, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his/her designated representative.

Guidance

A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation.

Applicability: All	**References:** ARS: CA-4; FISCAM: TSS-2.2.4; HSPD 7: F(19); IRS-1075: 6.3#1.1-2; NIST 800-53/53A: CA-4; PISP: 4.4.4	**Related Controls:** CA-2, CA-6, CA-7, SA-11, SI-2

ASSESSMENT PROCEDURE: CA-4.1

Assessment Objective

Determine if:
(i) the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and
(ii) the organization employs a security certification process in accordance with OMB policy and NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with security certification responsibilities.

CA-4(1) – Enhancement (High)

Control

Employ an independent certification agent or certification team to conduct an assessment of the information system security controls.

Guidance

An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment of the security controls be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

Applicability: All	**References:** ARS: CA-4(1); HSPD 7: F(19); NIST 800-53/53A: CA-4(1)	**Related Controls:** AC-9

ASSESSMENT PROCEDURE: CA-4(1).1

Assessment Objective

Determine if the organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; security accreditation package (including information system security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.

CA-4(CMS-1) – Enhancement (High)

Control

Document the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures.

Applicability: All	**References:** ARS: CA-4(CMS-1); HSPD 7: F(19), G(24)	**Related Controls:**

ASSESSMENT PROCEDURE: CA-4(CMS-1).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.

Interview: Organizational personnel with security certification responsibilities to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.

CA-5 – Plan of Action and Milestones (POA&M) (High)

Control

A POA&M shall be developed, implemented, and updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M shall document the planned, implemented, and evaluated corrective actions to repair deficiencies discovered during the security control assessment, and to reduce or eliminate any known vulnerability in the information system.

Personnel shall be designated to assign, track, and update risk mitigation efforts. Designated personnel shall define and authorize corrective action plans, and monitor corrective action progress.

Guidance

The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems. NIST SP 800-30 provides guidance on risk mitigation.

Applicability: All	References: ARS: CA-5; FISCAM: TSP-5.2; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4; NIST 800-53/53A: CA-5; PISP: 4.4.5	Related Controls: CA-7

ASSESSMENT PROCEDURE: CA-5.1

Assessment Objective

Determine if:
(i) the organization develops and updates at the organization-defined frequency, a plan of action and milestones for the information system; and
(ii) the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing plan of action and milestones; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.

CA-5(0) – Enhancement (High)

Control

Develop and submit a plan of action and milestones (POA&M) for any documented information system security finding within thirty (30) days of the final results for every internal / external audit / review or test (e.g., ST&E, penetration test). Update the POA&M monthly until all the findings are resolved.

Applicability: All	References: ARS: CA-5(0); HSPD 7: F(19), G(24); NIST 800-53/53A: CA-5; PISP: 4.4.5	Related Controls:

ASSESSMENT PROCEDURE: CA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Certification and accreditation policy and procedures; information system security plan (for organization-defined frequency of plan of action and milestones updates); security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.

CA-6 – Security Accreditation (High)

Control

Explicit authorization to operate the information system shall be received from the CMS CIO or his/her designated representative prior to the system being placed into operations. If the authorization is an interim approval to operate, then the authorization shall be granted based on the designated security category of the information system. An explicit corrective action plan shall be developed, implemented effectively, and monitored by the authorizing official. Re-authorization shall be obtained prior to continued operation:
4.4.6.1. At least every three (3) years;
4.4.6.2. When substantial changes are made to the system;
4.4.6.3. When changes in requirements result in the need to process data of a higher sensitivity;
4.4.6.4. When changes occur to authorizing legislation or federal requirements;
4.4.6.5. After the occurrence of a serious security violation which raises questions about the validity of an earlier certification; and
4.4.6.6. Prior to expiration of a previous accreditation.

Guidance

OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three (3) year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems.

Applicability: All	References: ARS: CA-6; FISCAM: TSP-5.1.3, TSP-5.2; HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6	Related Controls: CA-1, CA-2, CA-4, CA-7

ASSESSMENT PROCEDURE: CA-6.1

Assessment Objective

Determine if:

(i) the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization in accordance with organization-defined frequency, at least every three (3) years;
(ii) a senior organizational official signs and approves the security accreditation;
(iii) the security accreditation process employed by the organization is consistent with NIST SP 800-37; and
(iv) the organization updates the authorization when there is a significant change to the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST SP 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.
Interview: Organizational personnel with security accreditation responsibilities.

CA-6(0) – Enhancement (High)

Control

Information systems can only be accredited for a maximum period of three (3) years, after which the information system must be re-accredited.

Applicability: All	**References:** ARS: CA-6(0); HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6	**Related Controls:**

ASSESSMENT PROCEDURE: CA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST SP 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.
Interview: Organizational personnel with security accreditation responsibilities.

CA-7 – Continuous Monitoring (High)

Control

Security controls in CMS information systems shall be monitored on an on-going basis. Selection criteria for control monitoring shall be established and a subset of the security controls employed within information systems shall be selected for continuous monitoring purposes.

Guidance

Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2).
This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST SP 800-37 provides guidance on the continuous monitoring process. NIST SP 800-53 A provides guidance on the assessment of security controls.

Applicability: All	**References:** ARS: CA-7; HSPD 7: F(19); NIST 800-53/53A: CA-7; PISP: 4.4.7	**Related Controls:** CA-2, CA-4, CA-5, CA-6, CM-4, SI-2

ASSESSMENT PROCEDURE: CA-7.1

Assessment Objective

Determine if:
(i) the organization monitors the security controls in the information system on an ongoing basis; and
(ii) the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

Interview: Organizational personnel with continuous monitoring responsibilities.

ASSESSMENT PROCEDURE: CA-7.2

Assessment Objective

Determine if:
(i) the organization conducts security impact analyses on changes to the information system;
(ii) the organization documents and reports changes to or deficiencies in the security controls employed in the information system; and
(iii) the organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with continuous monitoring responsibilities.

CA-7(1) – Enhancement (High)

Control

The use of independent certification agents or teams is not required but, if used by the organization to monitor the security controls in the information system on an on-going basis, this can be used to satisfy ST&E requirements.

Guidance

The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle.

Applicability: All	**References:** ARS: CA-7(1); HSPD 7: F(19); NIST 800-53/53A: CA-7(1)	**Related Controls:** AC-9, CA-2

ASSESSMENT PROCEDURE: CA-7(1).1

Assessment Objective

Determine if the organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.(Optional)
Interview: Organizational personnel with continuous monitoring responsibilities.(Optional)

CA-7(CMS-1) – Enhancement (High)

Control

Continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and
(e) Status reporting.

Applicability: All	**References:** ARS: CA-7(CMS-1); HSPD 7: F(19)	**Related Controls:**

ASSESSMENT PROCEDURE: CA-7(CMS-1).1

Assessment Objective

Determine if:
(i) the organization monitors the security controls in the information system on an ongoing basis; and
(ii) the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records to determine continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;

(d) On-going assessment of security controls; and
(e) Status reporting.

Interview: Organizational personnel with continuous monitoring responsibilities to determine continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and
(e) Status reporting.

Configuration Management (CM) – *Operational*

CM-1 – Configuration Management Policy and Procedures (High)

Control

A CM process that includes the approval, testing, implementation, and documentation of changes shall be developed, documented, and implemented effectively to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with the organization's information technology architecture plans. Formally documented CM roles, responsibilities, procedures, and documentation shall be in place.

Guidance

The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CM-1; FISCAM: TCC-2.1.9, TCC-3.2.1, TCC-3.2.2, TCC-3.3.1, TSS-3.1.1, TSS-3.1.2, TSS-3.1.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-1; PISP: 4.5.1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents configuration management policy and procedures;
(ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review configuration management policy and procedures; and
(iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.
Interview: Organizational personnel with configuration management and control responsibilities.

ASSESSMENT PROCEDURE: CM-1.2

Assessment Objective

Determine if:
(i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.
Interview: Organizational personnel with configuration management and control responsibilities.

CM-2 – Baseline Configuration (High)

Control

A baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system shall be developed and documented. Procedures shall be developed, documented, and implemented effectively to maintain the baseline configuration. The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture.

Guidance

This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture.

Applicability: All	**References:** ARS: CM-2; HIPAA: 164.310(b); NIST 800-53/53A: CM-2; PISP: 4.5.2	**Related Controls:** CM-6, CM-8

ASSESSMENT PROCEDURE: CM-2.1

Assessment Objective

Determine if:
(i) the organization develops, documents, and maintains a baseline configuration of the information system;

(ii) the baseline configuration shows relationships among information system components and is consistent with the Federal Enterprise Architecture;
(iii) the baseline configuration provides the organization with a well-defined and documented specification to which the information system is built; and
(iv) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.

CM-2(1) – Enhancement (High)

Control

Update the baseline configuration of the information system as an integral part of information system component installations.

Applicability: All	**References:** ARS: CM-2(1); NIST 800-53/53A: CM-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CM-2(1).1

Assessment Objective

Determine if:
(i) the organization identifies the frequency of updates to the baseline configuration and instances that trigger configuration updates; and
(ii) the organization updates the baseline configuration of the information system as an integral part of information system component installations.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records.

CM-2(2) – Enhancement (High)

Control

Employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Applicability: All	**References:** ARS: CM-2(2); NIST 800-53/53A: CM-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CM-2(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.
Test: Automated mechanisms implementing baseline configuration maintenance.

CM-2(CMS-1) – Enhancement (High)

Control

Review and, if necessary, update the baseline configuration and any other system-related operations or security documentation at least once every year, and while planning major system changes / upgrades.

Applicability: All	**References:** ARS: CM-2(CMS-1); FISCAM: TSS-3.2.6	**Related Controls:**

ASSESSMENT PROCEDURE: CM-2(CMS-1).1

Assessment Objective

Determine if the organization develops, documents, and maintains a baseline configuration of the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records to determine the baseline configuration and any other system-related operations or security documentation are reviewed and updated at least once every year, and while planning major system changes / upgrades.
Interview: Organizational personnel with configuration management responsibilities to determine the baseline configuration and any other system-related operations or security documentation are reviewed and updated at least once every year, and while planning major system changes / upgrades.

CM-2(CMS-2) – Enhancement (High)

Control

Maintain an updated list of the information system's operations and security documentation.

Applicability: All	References: ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6	Related Controls:

ASSESSMENT PROCEDURE: CM-2(CMS-2).1

Assessment Objective

Determine if the organization updates the baseline configuration of the information system as an integral part of information system component installations.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records to determine an updated list of the information system's operations and security documentation is maintained.

Interview: Organizational personnel with configuration management responsibilities to determine an updated list of the information system's operations and security documentation is maintained.

CM-3 – Configuration Change Control (High)

Control

Change control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to control changes to the information system. Change request forms shall be used to document requests with related approvals. Change requests shall be approved by the Business Owner, or his/her designated representative, and other appropriate organization officials including, but not limited to, the system maintainer and information system support staff.

Test plans shall be developed and approved for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control) and shall include appropriate consideration of security. Test results shall be documented and appropriate responsive actions shall be taken based on the results.

Emergency changes for the CMS information system shall be documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration shall be documented appropriately and approved, and responsible personnel shall be notified for security analysis and follow-up.

Guidance

The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system.

Applicability: All	References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3	Related Controls: CM-4, CM-6, SI-2

ASSESSMENT PROCEDURE: CM-3.1

Assessment Objective

Determine if:
(i) the organization authorizes, documents, and controls changes to the information system;
(ii) the organization manages configuration changes to the information system using an organizationally approved process;
(iii) the organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws; and
(iv) the organization audits activities associated with configuration changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system configuration change control; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

CM-3(1) – Enhancement (High)

Control

Employ automated mechanisms to:
(a) Document proposed changes to the information system,
(b) Notify appropriate approval authorities,
(c) Identify approvals that have not been received in a timely manner,
(d) Inhibit change until necessary approvals are received, and
(e) Document completed changes to the information system.

Applicability: All	References: ARS: CM-3(1); FISCAM: TCC-1.2.1; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3(1)	Related Controls:

ASSESSMENT PROCEDURE: CM-3(1).1

Assessment Objective

Determine if:
(i) the organization employs automated mechanisms to document proposed changes to the information system;
(ii) the organization employs automated mechanisms to notify appropriate approval authorities;
(iii) the organization employs automated mechanisms to highlight approvals that have not been received in a timely manner;
(iv) the organization employs automated mechanisms to inhibit change until necessary approvals are received; and
(v) the organization employs automated mechanisms to document completed changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing configuration change control.

CM-3(FIS-1) – Enhancement (High)

Control

Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.

Applicability: All	**References:** FISCAM: TCC-2.1.11	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-1).1

Assessment Objective

Determine if the organization reviews production program changes for access and change control compliance.

Assessment Methods And Objects

Examine: Documentation of management or security administrator reviews.
Examine: Pertinent policies and procedures.
Interview: Information system management or security administrators.

CM-3(FIS-2) – Enhancement (High)

Control

Migration of tested and approved system software to production use is performed by an independent library control group.

Applicability: All	**References:** FISCAM: TSS-3.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-2).1

Assessment Objective

Determine if the organizational independent library control group migrates tested and approved software into production.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Supporting documentation for some system software migrations.
Interview: Management, systems programmers, and library control personnel, and determine who migrates approved system software to production libraries.

CM-3(FIS-3) – Enhancement (High)

Control

Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.

Applicability: All	**References:** FISCAM: TSS-3.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-3).1

Assessment Objective

Determine if the organization provides advance schedules to system users which minimize system software installation impacts.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Recent installations and determine whether scheduling and advance notification did occur.
Interview: Management and systems programmers about scheduling and giving advance notices when system software is installed.

CM-3(FIS-4) – Enhancement (High)

Control

Outdated versions of system software are removed from production libraries.

Applicability: All	References: FISCAM: TSS-3.2.3	Related Controls:

ASSESSMENT PROCEDURE: CM-3(FIS-4).1

Assessment Objective

Determine if the organization removes outdated versions of system software from the production libraries.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation for the removal of outdated versions from production libraries.

Interview: Management, systems programmers, and library control personnel, and determine whether outdated versions are removed from production libraries.

CM-4 – Monitoring Configuration Changes (High)

Control

Mechanisms to monitor change activity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to monitor information system changes and actions by privileged users. Security impact analyses shall be conducted after system changes are made to determine the IS-related effects of the changes. Activities associated with configuration changes to the information system shall be audited.

Guidance

Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system.

Applicability: All	References: ARS: CM-4; FISCAM: TCC-2.1.11, TCC-2.2.2, TCC-2.3.1, TCC-3.1, TSS-3.1.4; NIST 800-53/53A: CM-4; PISP: 4.5.4	Related Controls: CA-7, CM-3

ASSESSMENT PROCEDURE: CM-4.1

Assessment Objective

Determine if:

(i) the organization identifies the types of information system changes to be monitored;

(ii) the organization monitors changes to the information system; and

(iii) the organization conducts security impact analyses to assess the effects of the information system changes.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

CM-4(CMS-1) – Enhancement (High)

Control

When changes to the system occur, record the installation of information system components in the appropriate system documentation resource(s).

Applicability: All	References: ARS: CM-4(CMS-1); FISCAM: TCC-2.1.10, TCC-2.2.2, TCC-2.3.1, TCC-3.1, TSS-3.1.4	Related Controls:

ASSESSMENT PROCEDURE: CM-4(CMS-1).1

Assessment Objective

Determine if:

(i) the organization identifies the types of information system changes to be monitored;

(ii) the organization monitors changes to the information system; and

(iii) the organization conducts security impact analyses to assess the effects of the information system changes.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records to determine that when changes to the system occur, the installation of information system components is recorded in the appropriate system documentation resource(s).

Interview: Organizational personnel with information system monitoring responsibilities to determine that when changes to the system occur, the installation of information system components is

recorded in the appropriate system documentation resource(s).

CM-4(FIS-1) – Enhancement (High)

Control

Library management software is used to: (1) maintain program version numbers, (2) maintain creation/date information for production modules, (3) maintain copies of previous versions, and (4) control concurrent updates.

Applicability: All	**References:** FISCAM: TCC-3.1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-4(FIS-1).1

Assessment Objective

Determine if the organization uses library management software to: (1) maintain program version numbers, (2) maintain creation/date information for production modules, (3) maintain copies of previous versions, and (4) control concurrent updates.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Selection of programs maintained in the library and assess compliance with prescribed procedures.
Interview: Personnel responsible for library control.
Test: Verify how many prior versions of software modules are maintained.

CM-4(FIS-2) – Enhancement (High)

Control

Before and after images of program code are maintained and compared to ensure that only approved changes are made.

Applicability: All	**References:** FISCAM: TCC-3.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: CM-4(FIS-2).1

Assessment Objective

Determine if the organization ensures only approved program changes are made by maintaining and comparing before and after program code images.

Assessment Methods And Objects

Examine: For a selection of program changes, examine related documentation to verify that before and after images were compared.
Examine: Pertinent policies and procedures.
Interview: Application programmers, if available.

CM-5 – Access Restrictions for Change (High)

Control

Access control change mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to approve individual access privileges and to enforce physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.

Guidance

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

Applicability: All	**References:** ARS: CM-5; FISCAM: TCC-3.2.3, TCC-3.3.1, TSS-1.2.1, TSS-1.2.2, TSS-3.1.4, TSS-3.2.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-5; PISP: 4.5.5	**Related Controls:**

ASSESSMENT PROCEDURE: CM-5.1

Assessment Objective

Determine if:
(i) the organization maintains a list of qualified and authorized personnel permitted to access the information system for the express purpose of initiating changes;
(ii) the organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and
(iii) the organization generates, retains, and reviews records reflecting all such changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.
Test: Change control process and associated restrictions for changes to the information system.

CM-5(1) – Enhancement (High)

Control

Employ automated mechanisms to enforce access restrictions and to support auditing of the enforcement actions.

Applicability: All	References: ARS: CM-5(1); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-5(1)	Related Controls:

ASSESSMENT PROCEDURE: CM-5(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing access restrictions for changes to the information system.

CM-6 – Configuration Settings (High)

Control

Procedures shall be developed, documented, and implemented effectively to configure and benchmark information technology products in accordance with good security practice settings. Mandatory configuration settings for information technology products employed within the information system shall be established. The security settings of information technology products shall be configured to the most restrictive mode consistent with information system operational requirements, documented, and enforced in all components of the information system.

Guidance

Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems.

Applicability: All	References: ARS: CM-6; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6; PISP: 4.5.6	Related Controls: CM-2, CM-3, CM-8, SI-4

ASSESSMENT PROCEDURE: CM-6.1

Assessment Objective

Determine if:

(i) the organization establishes mandatory configuration settings for information technology products employed within the information system;

(ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;

(iii) the organization documents the configuration settings; and

(iv) the organization enforces the configuration settings in all components of the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST SP 800-70; other relevant documents or records.

Test: Information system configuration settings.

CM-6(1) – Enhancement (High)

Control

Employ automated mechanisms to centrally manage, apply, and verify configuration settings.

Applicability: All	References: ARS: CM-6(1); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6(1)	Related Controls:

ASSESSMENT PROCEDURE: CM-6(1).1

Assessment Objective

Determine if the information system employs automated mechanisms to centrally manage, apply, and verify configuration settings.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing the centralized management, application, and verification of configuration settings.

CM-6(CMS-1) – Enhancement (High)

Control

Configure the information system to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

Applicability: All	**References:** ARS: CM-6(CMS-1); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-6(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes mandatory configuration settings for information technology products employed within the information system;
(ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; and
(iii) the organization documents the configuration settings.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST SP 800-70; other relevant documents or records to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.
Interview: Organizational personnel with configuration management responsibilities to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.
Test: Information system to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

CM-7 – Least Functionality (High)

Control

Information systems shall be configured to provide only essential capabilities. The functions and services provided by CMS information systems shall be reviewed carefully to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol [VoIP], Instant Messaging [IM], File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP], file sharing). The use of those functions, ports, protocols, and/or services shall be prohibited and/or restricted.

Guidance

Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Applicability: All	**References:** ARS: CM-7; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7; PISP: 4.5.7	**Related Controls:**

ASSESSMENT PROCEDURE: CM-7.1

Assessment Objective

Determine if:
(i) the organization identifies prohibited or restricted functions, ports, protocols, and services for the information system;
(ii) the organization configures the information system to provide only essential capabilities; and
(iii) the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system for disabling or restriction of functions, ports, protocols, and services.

CM-7(0) – Enhancement (High)

Control

Configure the information system specifically to only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system / application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.

Applicability: All	**References:** ARS: CM-7(0); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7; PISP: 4.5.7	**Related Controls:**

ASSESSMENT PROCEDURE: CM-7(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan (for list of organization-defined prohibited or restricted functions, ports, protocols, and services for the information system); information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system configuration settings.

CM-7(1) – Enhancement (High)

Control

Review the information system every 365 days or on an incremental basis where all parts are addressed within a year, to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Applicability: All	**References:** ARS: CM-7(1); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CM-7(1).1

Assessment Objective

Determine if:
(i) the organization defines the frequency of the information system reviews to identify and eliminate unnecessary functions, ports, protocols, and services; and
(ii) the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services in accordance with the organizational defined frequency.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.

CM-8 – Information System Component Inventory (High)

Control

Procedures shall be developed, documented, and implemented effectively to document and maintain a current inventory of the information system's constituent components and relevant ownership information. The inventory of information system components shall include manufacturer, model / type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership.

Guidance

The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system.

Applicability: All	**References:** ARS: CM-8; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8; PISP: 4.5.8	**Related Controls:** CM-2, CM-6

ASSESSMENT PROCEDURE: CM-8.1

Assessment Objective

Determine if:
(i) the organization develops, documents, and maintains a current inventory of the components of the information system; and
(ii) the inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system inventory records; other relevant documents or records.

CM-8(1) – Enhancement (High)

Control

Update the information system component inventory as an integral part of component installations.

Applicability: All	**References:** ARS: CM-8(1); HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CM-8(1).1

Assessment Objective

Determine if the organization updates the inventory of information system components as an integral part of component installations.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records.

Interview: Organizational personnel with information system installation and inventory responsibilities.

CM-8(2) – Enhancement (High)

Control

Employ automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Applicability: All	**References:** ARS: CM-8(2); HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CM-8(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records.

Test: Automated mechanisms implementing information system component inventory management.

Contingency Planning (CP) – *Operational*

CP-1 – Contingency Planning Policy and Procedures (High)

Control

All major CMS information systems shall be covered by a CP that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

Guidance

The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-34 provides guidance on contingency planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CP-1; FISCAM: TSC-2.2.2; HIPAA: 164.308(a)(7)(i), 164.308(a)(7)(ii)(B); IRS-1075: 5.6.2.2#1.1; NIST 800-53/53A: CP-1; PISP: 4.6.1	**Related Controls:**

ASSESSMENT PROCEDURE: CP-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents contingency planning policy and procedures;
(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and
(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

ASSESSMENT PROCEDURE: CP-1.2

Assessment Objective

Determine if:
(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-2 – Contingency Plan (High)

Control

All major CMS information systems shall be covered by a CP, relative to the system security level, providing continuity of support in the event of a disruption of service. A CP for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A CP for the information system shall be consistent with NIST SP 800-34. Designated officials within the organization shall review and approve the CP and distribute copies of the plan to key contingency personnel.

Guidance

Contingency Plans consist of all components listed in the CMS Business Partners system Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.

Applicability: All	**References:** ARS: CP-2; FISCAM: TSC-1.1, TSC-1.2, TSC-1.3, TSC-2.1.2, TSC-3.1.1, TSC-3.1.2, TSC-3.1.3, TSC-3.1.4, TSC-3.2.3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.3; NIST 800-53/53A: CP-2; PISP: 4.6.2	**Related Controls:**

ASSESSMENT PROCEDURE: CP-2.1

Assessment Objective

Determine if:

(i) the organization develops and documents a contingency plan for the information system;
(ii) the contingency plan is consistent with NIST SP 800-34;
(iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure;
(iv) the contingency plan is reviewed and approved by designated organizational officials; and
(v) the organization disseminates the contingency plan to key contingency personnel.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; NIST SP 800-34; contingency plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-2.2

Assessment Objective

Determine if key contingency personnel and the key operating elements within the organization understand the contingency plan and are ready to implement the plan.

Assessment Methods And Objects

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-2(1) – Enhancement (High)

Control

Coordinate development of the Contingency Plan (CP) with parties responsible for related plans, such as the Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan (COOP), Business Recovery Plan, and Incident Response Plan.

Guidance

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

Applicability: All	**References:** ARS: CP-2(1); FISCAM: TSC-3.1.3; HIPAA: 164.308(a)(7)(ii)(E); HSPD 7: G(22)(i); NIST 800-53/53A: CP-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-2(1).1

Assessment Objective

Determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas.

CP-2(2) – Enhancement (High)

Control

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

Applicability: All	**References:** ARS: CP-2(2); HSPD 7: G(22)(i); NIST 800-53/53A: CP-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-2(2).1

Assessment Objective

Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-3 – Contingency Training (High)

Control

Operational and support personnel (including managers and users of the information system) shall receive training in contingency operations and understand their contingency roles and responsibilities with respect to the information system. Refresher training shall be provided to all contingency personnel.

Guidance

Managers, responsible for contingency operations, and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirmed that appropriate training has been completed.

Applicability: All	References: ARS: CP-3; FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3	Related Controls:

ASSESSMENT PROCEDURE: CP-3.1

Assessment Objective

Determine if:
(i) the organization provides contingency training to personnel with significant contingency roles and responsibilities;
(ii) the organization records the type of contingency training received and the date completed;
(iii) the organization defines frequency of refresher contingency training; and
(iv) the organization provides initial training and refresher training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan; other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

ASSESSMENT PROCEDURE: CP-3.2

Assessment Objective

Determine if contingency training material addresses the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.

CP-3(0) – Enhancement (High)

Control

Provide training every 365 days in contingency roles and responsibilities.

Applicability: All	References: ARS: CP-3(0); FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3	Related Controls:

ASSESSMENT PROCEDURE: CP-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan (for organization-defined frequency for refresher contingency training); other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-3(1) – Enhancement (High)

Control

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Applicability: All	References: ARS: CP-3(1); HSPD 7: G(22)(i); NIST 800-53/53A: CP-3(1)	Related Controls:

ASSESSMENT PROCEDURE: CP-3(1).1

Assessment Objective

Determine if:
(i) the organization incorporates simulated events into contingency training; and
(ii) the training is effective in getting organizational personnel to respond as expected to simulated crisis situations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-3(2) – Enhancement (High)

Control

Employ automated mechanisms to provide thorough and realistic training environments.

Applicability: All	References: ARS: CP-3(2); HSPD 7: G(22)(i); NIST 800-53/53A: CP-3(2)	Related Controls:

ASSESSMENT PROCEDURE: CP-3(2).1

Assessment Objective

Determine if:
(i) the organization employs automated mechanisms for contingency training; and
(ii) the automated mechanisms improve the effectiveness of the contingency training.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; automated mechanisms supporting contingency training; contingency training curriculum; contingency training material; other relevant documents or records.(Optional)

Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.(Optional)

CP-4 – Contingency Plan Testing and Exercises (High)

Control

CPs shall be tested and/or exercised at least every 365 days using defined tests and exercises, such as the tabletop test in accordance with current CMS Procedures, to determine the plans' effectiveness and readiness to execute the plan. Test / exercise results shall be documented and reviewed by appropriate organization officials. Reasonable and appropriate corrective actions shall be initiated to close or reduce the impact of CP failures and deficiencies.

Guidance

There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Applicability: All	References: ARS: CP-4; FISCAM: TSC-1.1, TSC-4.1, TSC-4.2.1, TSC-4.2.2; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2; NIST 800-53/53A: CP-4; PISP: 4.6.4	Related Controls:

ASSESSMENT PROCEDURE: CP-4.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of contingency plan tests and/or exercises;
(ii) the organization defines the set of contingency plan tests and/or exercises;
(iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;
(iv) the organization documents the results of contingency plan testing/exercises; and
(v) the organization reviews the contingency plan test/exercise results and takes corrective actions.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-4.2

Assessment Objective

Determine if the contingency plan tests/exercises address key aspects of the plan.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records.

CP-4(0) – Enhancement (High)

Control

The CP must be current and executable, tested using a combination of tabletop exercises and operational tests every 365 days, and updated as needed.

Applicability: All	References: ARS: CP-4(0); FISCAM: TSC-4.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-4; PISP: 4.6.4	Related Controls:

ASSESSMENT PROCEDURE: CP-4(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan (for the organization-defined frequency of contingency plan tests and/or exercises and the list of the organization-defined contingency plan tests and/or exercises); contingency plan testing and/or exercise documentation; other relevant documents or records.

CP-4(1) – Enhancement (High)

Control

Coordinate testing and exercising of CP with parties responsible for related plans, such as:
(a) Business Continuity Plan,
(b) Disaster Recovery Plan,
(c) Continuity of Operations Plan,
(d) Business Recovery Plan, and
(e) Incident Response Plan.

Guidance

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

Applicability: All	**References:** ARS: CP-4(1); HSPD 7: G(22)(i); NIST 800-53/53A: CP-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-4(1).1

Assessment Objective

Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities.

CP-4(2) – Enhancement (High)

Control

Test / exercise the CP at the alternate processing site to evaluate the site's capabilities to support contingency operations.

Applicability: All	**References:** ARS: CP-4(2); HSPD 7: G(22)(i); NIST 800-53/53A: CP-4(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-4(2).1

Assessment Objective

Determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records.

CP-4(3) – Enhancement (High)

Control

Employ automated mechanisms to more thoroughly and effectively test / exercise the CP by providing more complete coverage of contingency issues, selecting more realistic test / exercise scenarios and environments, and more effectively stressing the information system and supported missions.

Applicability: All	**References:** ARS: CP-4(3); FISCAM: TSC-4.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-4(3)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-4(3).1

Assessment Objective

Determine if:
(i) the organization employs automated mechanisms for contingency plan testing/exercises; and
(ii) the automated mechanisms improve the effectiveness of the contingency plan testing/exercises.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; automated mechanisms supporting contingency plan testing/exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.(Optional)

CP-5 – Contingency Plan Update (High)

Control

CPs shall be reviewed at least every 365 days and, if necessary, revised to address system / organizational changes and/or any problems encountered during plan implementation, execution, or testing.

Guidance

Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Applicability: All	**References:** ARS: CP-5; FISCAM: TSC-1.1, TSC-3.1.5; HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	**Related Controls:**

ASSESSMENT PROCEDURE: CP-5.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of contingency plan reviews and updates;
(ii) the organization updates the contingency plan in accordance with organization-defined frequency, at least annually; and
(iii) the revised plan addresses the system/organizational changes identified by the organization or any problems encountered by the organization during plan implementation, execution, and testing.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-5.2

Assessment Objective

Determine if the organization communicates necessary changes to the contingency plan to other organizational elements with related plans.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records.
Interview: Organizational personnel with contingency plan update responsibilities; organizational personnel with mission-related and operational responsibilities.

CP-5(0) – Enhancement (High)

Control

Review the CP at least every 365 days and update, as necessary, to address: system, organizational, or facility changes; problems encountered during plan implementation, execution, or testing; or other conditions that may impact the system CP.

Applicability: All	**References:** ARS: CP-5(0); HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	**Related Controls:**

ASSESSMENT PROCEDURE: CP-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan (for organization-defined frequency of contingency plan reviews and updates); other relevant documents or records.
Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records.
Interview: Organizational personnel with contingency plan review and update responsibilities; organizational personnel with mission-related and operational responsibilities.

CP-6 – Alternate Storage Site (High)

Control

Agreements with an alternate storage site shall be established and implemented effectively to permit the storage of CMS information system backup information. Copies of the current CP shall be stored in a secure location at an alternate site accessible by management and other key personnel. Procedures shall be developed, documented, and implemented effectively to respond to contingencies by ensuring separation of routine information system operations and the alternate storage site.

Guidance

The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives

and recovery point objectives.

Applicability: All	References: ARS: CP-6; IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6; PISP: 4.6.6	Related Controls:

ASSESSMENT PROCEDURE: CP-6.1

Assessment Objective

Determine if:
(i) the organization identifies an alternate storage site; and
(ii) alternate storage site agreements are currently in place (if needed) to permit storage of information system backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-6.2

Assessment Objective

Determine if the alternate storage site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information consistent with the organization's recovery time objectives and recovery point objectives.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.
Interview: Organizational personnel with alternate storage site responsibilities.

CP-6(1) – Enhancement (High)

Control

Ensure that the alternate storage site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.

Applicability: All	References: ARS: CP-6(1); FISCAM: TSC-2.1.3; IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(1)	Related Controls:

ASSESSMENT PROCEDURE: CP-6(1).1

Assessment Objective

Determine if:
(i) the contingency plan identifies the primary storage site hazards; and
(ii) the alternate storage site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

CP-6(2) – Enhancement (High)

Control

Ensure that the alternate storage site is configured to facilitate timely and effective recovery operations.

Applicability: All	References: ARS: CP-6(2); IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(2)	Related Controls:

ASSESSMENT PROCEDURE: CP-6(2).1

Assessment Objective

Determine if the alternate storage site is configured to enable timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives) in accordance with the provisions of alternate storage site agreements.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate storage site; other relevant documents or records.

CP-6(3) – Enhancement (High)

Control

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and document explicit mitigation actions.

Applicability: All	References: ARS: CP-6(3); IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(3)	Related Controls:

ASSESSMENT PROCEDURE: CP-6(3).1

Assessment Objective

Determine if:
(i) the contingency plan identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and

(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

CP-7 – Alternate Processing Site (High)

Control

Agreements with an alternate processing site shall be established and implemented to permit the resumption of CMS information system operations for mission critical business functions when the primary processing capabilities are unavailable, and the CP calls for application recovery in place of other accepted processes. Procedures shall be developed, documented, and implemented effectively to establish contingency activities and responsibilities.

Guidance

Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives.

Applicability: All	**References:** ARS: CP-7; FISCAM: TSC-3.2.1; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7; PISP: 4.6.7	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7.1

Assessment Objective

Determine if:

(i) the organization identifies an alternate processing site;

(ii) the organization defines the time period within which processing must be resumed at the alternate processing site; and

(iii) alternate processing site agreements are currently in place (if needed) to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-7.2

Assessment Objective

Determine if the alternate processing site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

Interview: Organizational personnel with alternate processing site responsibilities.

CP-7(0) – Enhancement (High)

Control

Ensure all equipment and supplies required for resuming information system operations for critical functions within twelve (12) hours after COOP activation are available at the alternate processing site, or contracts are in place to support delivery to the site.

Applicability: All	**References:** ARS: CP-7(0); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7; PISP: 4.6.7	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan (for organization-defined time period within which processing must be resumed at the alternate processing site); other relevant documents or records.

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

Interview: Organizational personnel with alternate processing site responsibilities.

CP-7(1) – Enhancement (High)

Control

Ensure the alternate processing site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.

Applicability: All	**References:** ARS: CP-7(1); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(1).1

Assessment Objective

Determine if:
(i) the contingency plan identifies the primary processing site hazards; and
(ii) the alternate processing site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

CP-7(2) – Enhancement (High)

Control

Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Applicability: All	**References:** ARS: CP-7(2); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(2).1

Assessment Objective

Determine if:
(i) the contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and
(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

CP-7(3) – Enhancement (High)

Control

Ensure alternate processing site agreements contain appropriate priority-of-service provisions.

Applicability: All	**References:** ARS: CP-7(3); FISCAM: TSC-3.2.1; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(3)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(3).1

Assessment Objective

Determine if alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records.

CP-7(4) – Enhancement (High)

Control

Ensure the alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.

Applicability: All	**References:** ARS: CP-7(4); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(4)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(4).1

Assessment Objective

Determine if alternate processing site agreements specify the requirements needed to support the minimum required operational capability of the organization.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-7(4).2

Assessment Objective

Determine if the alternate processing site is configured to support the minimum required operational capability of the organization and is ready to use as the operational site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records.
Test: Information system at the alternate processing site.

CP-8 – Telecommunications Services (High)

Control

Necessary agreements shall be established and implemented for alternate communications services capable of restoring adequate communications to accomplish mission critical functions when the primary operations and communications capabilities are unavailable.

Guidance

In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).

Applicability: All	**References:** ARS: CP-8; FISCAM: TSC-3.2.2; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8; PISP: 4.6.8	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8.1

Assessment Objective

Determine if:
(i) the organization identifies primary and alternate telecommunications services to support the information system;
(ii) the organization defines the time period within which resumption of information system operations must take place; and
(iii) alternate telecommunications service agreements are in place to permit the resumption of telecommunications services for critical mission/business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; information system security plan; primary and alternate telecommunications service agreements; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-8.2

Assessment Objective

Determine if:
(i) telecommunications services supporting the organization are used for national security emergency preparedness; and
(ii) a common carrier provides telecommunications services.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

CP-8(0) – Enhancement (High)

Control

Resume system operations for critical functions within twelve (12) hours when the primary telecommunications capabilities are unavailable.

Applicability: All	**References:** ARS: CP-8(0); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8; PISP: 4.6.8	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; information system security plan (for organization-defined time period within which resumption of information system operations must take place); primary and alternate telecommunications service agreements; other relevant documents or records.
Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

CP-8(1) – Enhancement (High)

Control

Ensure agreements with primary and alternate telecommunication service providers include priority-of-service provisions.

Applicability: All	**References:** ARS: CP-8(1); FISCAM: TSC-3.2.2; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8(1).1

Assessment Objective

Determine if primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the availability requirements defined in the organization's contingency plan.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

CP-8(2) – Enhancement (High)

Control

Ensure alternate telecommunication providers do not share a single point of failure with primary telecommunications services.

Applicability: All	**References:** ARS: CP-8(2); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8(2).1

Assessment Objective

Determine if primary and alternate telecommunications services share a single point of failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

CP-8(3) – Enhancement (High)

Control

Ensure alternate telecommunications service providers are sufficiently separated from the primary telecommunications services, to prevent susceptibility to the same hazards.

Applicability: All	**References:** ARS: CP-8(3); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(3)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8(3).1

Assessment Objective

Determine if the alternate telecommunications service provider's site is sufficiently separated from the primary telecommunications service provider's site so as not to be susceptible to the same hazards identified at the primary site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; alternate telecommunications service provider's site; primary telecommunications service provider's site; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

CP-8(4) – Enhancement (High)

Control

Ensure that primary and alternate telecommunication service providers have adequate CPs.

Applicability: All	**References:** ARS: CP-8(4); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(4)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8(4).1

Assessment Objective

Determine if the contingency plans for the primary and alternate telecommunications service providers are sufficient to meet the needs of the organization.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers.

Test: Operational capability by exercising priority-of-service provisions of alternate telecommunications service agreements.

CP-9 – Information System Backup (High)

Control

Backup mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable the backing-up of user-level and system-level information (including system state information) contained in the CMS information system. The frequency of information system backups and the transfer rate of backup information to an alternate storage site (if so designated) shall be consistent with the CMS recovery time objectives and recovery point objectives.

Mechanisms shall provide for sufficient backup storage capability. Checkpoint capabilities shall be part of any backup operation that updates files and consumes large amounts of information system time. Backup copies of CMS data shall be created on a regular basis, and appropriate safeguards shall be implemented to protect the technical and physical security of backup media at the storage location. Where appropriate, backup copies of all other forms of data, including paper records, shall be created based upon an assessment of the level of data criticality and the corresponding risk of

data loss.

Guidance

The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time. The protection of system backup information while in transit is beyond the scope of this control.

Applicability: All	References: ARS: CP-9; FISCAM: TSC-2.1.1, TSC-2.1.3; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	Related Controls: MA-CMS-1, MA-CMS-2, MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of information systems backups;
(ii) the organization defines the user-level and system-level information (including system state information) that is required to be backed up; and
(iii) the organization identifies the location(s) for storing backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records.

ASSESSMENT PROCEDURE: CP-9.2

Assessment Objective

Determine if:
(i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency;
(ii) the organization stores backup information in designated locations in accordance with information system backup procedures; and
(iii) the organization protects backup information at the designated storage locations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records.

CP-9(0) – Enhancement (High)

Control

Perform full backups to separate media every other day. Perform incremental or differential backups to separate media on the intervening day. Backups to include user-level and system-level information (including system state information). Three generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time and action.

Applicability: All	References: ARS: CP-9(0); HIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	Related Controls:

ASSESSMENT PROCEDURE: CP-9(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for information system backup); backup storage location(s); other relevant documents or records.

CP-9(1) – Enhancement (High)

Control

Test backup information to verify media reliability and information integrity, following each backup.

Applicability: All	References: ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1)	Related Controls:

ASSESSMENT PROCEDURE: CP-9(1).1

Assessment Objective

Determine if:

(i) the organization defines the frequency of information system backup testing;
(ii) the organization conducts information system backup testing within the organization-defined frequency; and
(iii) testing results verify backup media reliability and information integrity.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; information system backup test results; backup storage location(s); other relevant documents or records.

CP-9(2) – Enhancement (High)

Control

Use select backup information to restore information systems as part of the Contingency Plan testing.

Applicability: All	**References:** ARS: CP-9(2); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-9(2).1

Assessment Objective

Determine if the organization uses selected backup information in the restoration of information system functions as part of contingency plan testing.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system backup test results; contingency plan test results; other relevant documents or records.

CP-9(3) – Enhancement (High)

Control

Ensure that backup copies of the operating system and other critical information system software are stored at a separate facility or in a fire-rated container that is not collocated with operational software.

Applicability: All	**References:** ARS: CP-9(3); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(3)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-9(3).1

Assessment Objective

Determine if the organization stores backup copies of operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; backup storage location(s); other relevant documents or records.

CP-9(4) – Enhancement (High)

Control

Protect backup information from unauthorized modification.

Guidance

The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control.

Applicability: All	**References:** ARS: CP-9(4); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(4)	**Related Controls:** MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9(4).1

Assessment Objective

Determine if the organization employs appropriate mechanisms to protect the integrity of information system backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; backup storage location(s); information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with information system backup responsibilities.

CP-9(PII-1) – Enhancement (High)

Control

Insure that a current, retrievable, copy of PII is available before movement of servers.

Applicability: All	**References:** HIPAA: 164.310(d)(2)(iv)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-9(PII-1).1

Assessment Objective

Determine if the organization ensures a current and retrievable copy of PII is available before movement of servers.

Assessment Methods And Objects

Examine: PII Server Movement Plan is addresses in the COOP and backup procedures are available. A current copy of PII is available.
Interview: Organizational personnel with PII backup responsibilities to determine if the PII copy is current and retrievable.
Test: Following the data backup and reconstitution procedures for PII, determine if the current copy is retrievable.

CP-10 – Information System Recovery and Reconstitution (High)

Control

Information system recovery and reconstitution mechanisms with supporting procedures shall be developed, documented, and implemented effectively to allow the CMS information system to be recovered and reconstituted to a known secure state after a disruption or failure. Recovery of CMS information systems after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

Guidance

Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Applicability: All	**References:** ARS: CP-10; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10; PISP: 4.6.10	**Related Controls:**

ASSESSMENT PROCEDURE: CP-10.1

Assessment Objective

Determine if the organization identifies the means for capturing the information system's operational state including appropriate system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-10.2

Assessment Objective

Determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.
Test: Automated mechanisms implementing information system recovery and reconstitution operations.

CP-10(0) – Enhancement (High)

Control

Secure information system recovery and reconstitution includes, but not limited to:
(a) Reset all system parameters (either default or organization-established),
(b) Reinstall patches,
(c) Reestablish configuration settings,
(d) Reinstall application and system software, and
(e) Fully test the system.

Applicability: All	**References:** ARS: CP-10(0); NIST 800-53/53A: CP-10; PISP: 4.6.10	**Related Controls:**

ASSESSMENT PROCEDURE: CP-10(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing information system recovery and reconstitution operations.

CP-10(1) – Enhancement (High)		
Control Perform full recovery and reconstitution of the information system as part of CP testing.		
Applicability: All	**References:** ARS: CP-10(1); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10(1)	**Related Controls:**
ASSESSMENT PROCEDURE: CP-10(1).1		
Assessment Objective Determine if the organization includes a full recovery and reconstitution of the information system as part of contingency plan testing. **Assessment Methods And Objects** **Examine:** Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan test procedures; contingency plan test results; other relevant documents or records. **Interview:** Organizational personnel with information system recovery and reconstitution responsibilities; organizational personnel with contingency testing responsibilities.		

Identification and Authentication (IA) – *Technical*

IA-1 – Identification and Authentication Policy and Procedures (High)

Control

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

Guidance

The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and SP 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**References:** ARS: IA-1; IRS-1075: 5.6.3.1#1.1; NIST 800-53/53A: IA-1; PISP: 4.7.1	**Related Controls:**

ASSESSMENT PROCEDURE: IA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents identification and authentication policy and procedures;
(ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review identification and authentication policy and procedures; and
(iv) the organization updates identification and authentication policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.
Interview: Organizational personnel with identification and authentication responsibilities.

ASSESSMENT PROCEDURE: IA-1.2

Assessment Objective

Determine if:
(i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.
Interview: Organizational personnel with identification and authentication responsibilities.

IA-2 – User Identification and Authentication (High)

Control

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique IA of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

Guidance

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in SP 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST SP 800-63 level 1 compliant. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST SP 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals.

Applicability: All	**References:** ARS: IA-2; FISCAM: TAC-3.2.A.4, TAN-2.1.4; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 5.6.3.1#1.2, 5.6.3.3#2.3; NIST 800-53/53A: IA-2; PISP: 4.7.2	**Related Controls:** AC-14, AC-17, MA-4

ASSESSMENT PROCEDURE: IA-2.1

Assessment Objective

Determine if:
(i) the information system uniquely identifies and authenticates users (or processes acting on behalf of users); and
(ii) authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63 and e-authentication risk assessment results.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; e-authentication risk assessment results; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(1) – Enhancement (High)

Control

Not applicable.

Applicability: All	**References:** ARS: IA-2(1); FISCAM: TAN-2.1.7; HIPAA: 164.312(d); IRS-1075: 5.6.3.1#1.2	**Related Controls:**

IA-2(2) – Enhancement (High)

Control

Employ multifactor authentication for local system access that is at least NIST SP 800-63 level 3 compliant.

Applicability: All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC	**References:** ARS: IA-2(2); NIST 800-53/53A: IA-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: IA-2(2).1

Assessment Objective

Determine if:
(i) the organization defines the NIST SP 800-63 authentication levels for the information system; and
(ii) the information system employs multifactor authentication for local system access that is NIST SP 800-63 compliant in accordance with the organizational selection of level 3 or level 4.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-2(3) – Enhancement (High)

Control

Employ multifactor authentication for remote system access that is NIST SP 800-63 level 4 compliant.

Applicability: All	**References:** ARS: IA-2(3); FISCAM: TAN-2.1.7; NIST 800-53/53A: IA-2(3)	**Related Controls:**

ASSESSMENT PROCEDURE: IA-2(3).1

Assessment Objective

Determine if:
(i) the organization defines the NIST SP 800-63 authentication levels for the information system; and
(ii) the information system employs multifactor authentication for remote system access that is NIST SP 800-63 level 4 compliant.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-2(CMS-1) – Enhancement (High)		
Control Require the use of unique user identifiers and system and/or network authenticators.		
Applicability: All	**References:** ARS: IA-2(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4, TAN-2.1.4, TAN-2.1.7; IRS-1075: 5.6.3.1#1.2	**Related Controls:**
ASSESSMENT PROCEDURE: IA-2(CMS-1).1		
Assessment Objective Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users). **Assessment Methods And Objects** **Examine:** Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine the use of unique user identifiers and system and/or network authenticators is required. **Interview:** Organizational personnel with identification and authentication responsibilities to determine the use of unique user identifiers and system and/or network authenticators is required. **Test:** Automated mechanisms implementing identification and authentication capability for the information system to determine the use of unique user identifiers and system and/or network authenticators is required.		
IA-2(CMS-2) – Enhancement (High)		
Control All passwords shall be encrypted in transit and at rest.		
Applicability: All	**References:** ARS: IA-2(CMS-2); FISCAM: TAC-3.2.A.1, TAC-3.2.A.7; IRS-1075: 5.6.3.1#1.2	**Related Controls:**
ASSESSMENT PROCEDURE: IA-2(CMS-2).1		
Assessment Objective Determine if authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63. **Assessment Methods And Objects** **Examine:** Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine all passwords are required to be encrypted in transit and at rest. **Interview:** Organizational personnel with identification and authentication responsibilities to determine to determine all passwords are required to be encrypted in transit and at rest. **Test:** Automated mechanisms implementing identification and authentication capability for the information system to determine all passwords are required to be encrypted in transit and at rest.		
IA-2(CMS-3) – Enhancement (High)		
Control Help desk support requires user identification for any transaction that has information security implications.		
Applicability: All	**References:** ARS: IA-2(CMS-3)	**Related Controls:**
ASSESSMENT PROCEDURE: IA-2(CMS-3).1		
Assessment Objective Determine if authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63. **Assessment Methods And Objects** **Examine:** Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine help desk support requires user identification for any transaction that has information security implications. **Interview:** Organizational personnel with identification and authentication responsibilities to determine to determine help desk support requires user identification for any transaction that has information security implications. **Test:** Automated mechanisms implementing identification and authentication capability for the information system to determine help desk support requires user identification for any transaction that has information security implications.		
IA-3 – Device Identification and Authentication (High)		
Control Automated mechanisms shall be used to enable IA of the CMS information system being used and to which a connection is being made before establishing a connection.		

Guidance

The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802. 1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Applicability: All	**References:** ARS: IA-3; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	**Related Controls:**

ASSESSMENT PROCEDURE: IA-3.1

Assessment Objective

Determine if:
(i) the organization defines specific devices requiring identification and authentication before establishing connections to the information system; and
(ii) the information system identifies and authenticates specific devices identified by the organization before establishing connections.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing device identification and authentication.

IA-3(0) – Enhancement (High)

Control

Implement an information system that uses either a shared secret or digital certificate to identify and authenticate specific devices before establishing a connection.

Applicability: All	**References:** ARS: IA-3(0); IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	**Related Controls:**

ASSESSMENT PROCEDURE: IA-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; information system design documentation; procedures addressing device identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing device identification and authentication.

IA-4 – Identifier Management (High)

Control

Procedures shall be developed, documented, and implemented effectively to manage user identifiers. The procedures shall address processes and controls for:
4.7.4.1. Identifying each user uniquely;
4.7.4.2. Verifying the identity of each user;
4.7.4.3. Receiving authorization to issue a user identifier from an appropriate organization official;
4.7.4.4. Ensuring that the user identifier is issued to the intended party;
4.7.4.5. Disabling user identifier after a specific period of inactivity; and
4.7.4.6. Archiving user identifiers.

Reviews and validation of system users' accounts shall be conducted to ensure the continued need for access to a system. Identifier management shall not be applicable to shared information system accounts (i.e., guest and anonymous).

Guidance

Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors.

Applicability: All	**References:** ARS: IA-4; FISCAM: TAC-3.2.A.4, TAN-2.1.4; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-4; PISP: 4.7.4	**Related Controls:**

ASSESSMENT PROCEDURE: IA-4.1

Assessment Objective

Determine if:
(i) the organization manages user identifiers by uniquely identifying each user;
(ii) the organization manages user identifiers by verifying the identity of each user;

(iii) the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official;
(iv) the organization manages user identifiers by issuing the identifier to the intended party;
(v) the organization defines the time period of inactivity after which a user identifier is to be disabled;
(vi) the organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and
(vii) the organization manages user identifiers by archiving identifiers.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Identity verification capability for the information system and for organizational facilities.

ASSESSMENT PROCEDURE: IA-4.2

Assessment Objective

Determine if the organization uses a Personal Identity Verification (PIV) card token to uniquely identify and authenticate federal employees and contractors in accordance with FIPS 201 and NIST SP 800-73, 800-76, and 800-78.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST SP 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Identity verification capability for the information system and for organizational facilities.

IA-4(0) – Enhancement (High)

Control

Disable user identifiers after 90 days of inactivity and delete disabled accounts during annual re-certification process.

Applicability: All	**References:** ARS: IA-4(0); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.1#2, 5.6.3.2#2.1; NIST 800-53/53A: IA-4; PISP: 4.7.4	**Related Controls:** AC-2(3)

ASSESSMENT PROCEDURE: IA-4(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Identity verification capability for the information system and for organizational facilities.
Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST SP 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

IA-4(CMS-1) – Enhancement (High)

Control

Require system administrator to maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.

Applicability: All	**References:** ARS: IA-4(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4; IRS-1075: 5.6.3.1#2	**Related Controls:** AC-2(CMS-2)

ASSESSMENT PROCEDURE: IA-4(CMS-1).1

Assessment Objective

Determine if the organization manages user identifiers by uniquely identifying each user.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.
Interview: Organizational personnel with identification and authentication responsibilities to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.
Test: Identity verification capability for the information system and for organizational facilities to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.

IA-4(CMS-2) – Enhancement (High)		
Control For non-CMS entities to issue user identifiers, receive prior written approval from the CIO or his/her designated representative.		
Applicability: All	**References:** ARS: IA-4(CMS-2)	**Related Controls:**
ASSESSMENT PROCEDURE: IA-4(CMS-2).1		
Assessment Objective Determine if responsible parties within the organization periodically review identification and authentication policy and procedures. **Assessment Methods And Objects** **Examine:** Identification and authentication policy and procedures; other relevant documents or records to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers. **Interview:** Organizational personnel with identification and authentication management responsibilities to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers.		
IA-4(FIS-1) – Enhancement (High)		
Control Personnel files are matched with actual system users to remove terminated or transferred employees from the system.		
Applicability: All	**References:** FISCAM: TAC-3.2.A.6	**Related Controls:**
ASSESSMENT PROCEDURE: IA-4(FIS-1).1		
Assessment Objective Determine if the organizational personnel files are automatically [or manually] matched with actual system users to remove terminated or transferred employees from the system. **Assessment Methods And Objects** **Examine:** Documentation of such comparisons. **Examine:** Pertinent policies and procedures. **Interview:** Security managers.		
IA-5 – Authenticator Management (High)		
Control Procedures shall be developed, documented, and implemented effectively to manage user authenticators. The procedures shall address processes and controls for: initial authenticator content; distribution for new, lost, compromised, or damaged authenticators; revocation of authenticators; changing default authenticators; and changing / refreshing authenticators at specified intervals. Users shall not loan or share authenticators with other users. Lost or compromised authenticators shall be reported immediately to appropriate authority. Selection of passwords or other authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS System Security Level of the information system. Automated mechanisms shall be in place for password-based authentication, to ensure that the information system: 4.7.5.1. Protects passwords from unauthorized disclosure and modification when stored and transmitted; 4.7.5.2. Prohibits passwords from being displayed when entered; 4.7.5.3. Enforces automatic expiration of passwords; 4.7.5.4. Prohibits password reuse for a specified number of generations; and 4.7.5.5. Enforces periodic password changes.		
Guidance Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication.		
Applicability: All	**References:** ARS: IA-5; FISCAM: TAC-3.2.A.1, TAC-3.2.A.3; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	**Related Controls:** AC-11(0), AC-CMS-1(CMS-2)

ASSESSMENT PROCEDURE: IA-5.1

Assessment Objective

Determine if:
(i) the organization manages information system authenticators by defining initial authenticator content;
(ii) the organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;
(iii) the organization manages information system authenticators by changing default authenticators upon information system installation; and
(iv) the organization manages information system authenticators by changing/refreshing authenticators periodically.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Automated mechanisms implementing authenticator management functions.

IA-5(0) – Enhancement (High)

Control

For password-based authentication:
(a) Protect passwords from disclosure or modification when stored or transmitted,
(b) Prevent passwords from being displayed when entered,
(c) When using passwords in connection with e-authentication, refer to ARS Appendix A, e-Authentication Standards for further guidance,
(d) Force users to select a password comprising a minimum of eight (8) alphanumeric and/or special characters with a number embedded in the password,
(e) Automatically force users (including administrators) to change account and system account passwords every sixty (60) days,
(f) Automatically force users to select six (6) unique passwords prior to reusing a previous one, and
(g) Enforce password lifetime restrictions within a minimum of one (1) day and maximum of sixty (60) days.

Applicability: All	**References:** ARS: IA-5(0); HIPAA: 164.308(a)(5)(ii)(D); IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Automated mechanisms implementing authenticator management functions.

IA-5(FIS-1) – Enhancement (High)

Control

For devices such as tokens or key cards, users: (1) maintain possession of their individual tokens, cards, etc., and (2) understand that they must not loan or share these with others, and must report lost items immediately.

Applicability: All	**References:** FISCAM: TAC-3.2.A.8	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(FIS-1).1

Assessment Objective

Determine if:
(i) the organizational users maintain possession of their individual devices such as tokens or key cards, etc.; and
(ii) the organizational users understand they must not loan or share their individual tokens, cards, etc., and report lost items immediately.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Token or key card acknowledgment forms.
Interview: Token and/or key card users.

IA-5(DIR-1) – Enhancement (High)

Control

For password-based authentication, passwords are:

(a) unique for specific individuals, not groups;
(b) controlled by the assigned user and not subject to disclosure;
(c) not displayed when entered;
(d) changed every 60 days, when an individual changes positions, or when security is breached;
(e) at least 8 characters in length;
(f) must include at least one number, one upper and lower case character, and one special character;
(g) prohibited from reuse for at least 6 generations;
(h) prohibited from being changed more than once in a 24-hour period; and
(i) all passwords are encrypted in transit and at rest. The use of dictionary names or words as passwords is prohibited.

Applicability: All	**References:** FISCAM: TAC-3.2.A.1, TAC-3.2.A.2, TAN-2.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(DIR-1).1

Assessment Objective

Determine if the organization effectively uses password and user identification as one tool for security in-depth.

Assessment Methods And Objects

Examine: Password and user identification policy and acceptable user training policy for completeness in meeting the CMS password controls.
Interview: A sampling of users know the organization's policy for password and user system identification.
Test: Using an appropriate system guide or script check the system password configuration:
(a) unique for specific individuals, not groups;
(b) controlled by the assigned user and not subject to disclosure;
(c) not displayed when entered;
(d) changed every 60 days, when an individual changes positions, or when security is breached;
(e) at least 8 characters in length;
(f) must include at least one number, one upper and lower case character, and one special character;
(g) prohibited from reuse for at least 6 generations;
(h) prohibited from being changed more than once in a 24-hour period; and
(i) all passwords are encrypted in transit and at rest. The use of dictionary names or words as passwords is prohibited.

IA-6 – Authenticator Feedback (High)

Control

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to obscure feedback to users during the authentication process to protect the information from possible exploitation / use by unauthorized individuals.

Guidance

The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Applicability: All	**References:** ARS: IA-6; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-6; PISP: 4.7.6	**Related Controls:**

ASSESSMENT PROCEDURE: IA-6.1

Assessment Objective

Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing authenticator feedback.

IA-6(0) – Enhancement (High)

Control

Configure the information system to obscure passwords during the authentication process (e.g., display asterisks).

Applicability: All	**References:** ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6	**Related Controls:**

ASSESSMENT PROCEDURE: IA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing authenticator feedback.

IA-7 – Cryptographic Module Authentication (High)

Control

Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Guidance

The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	**References:** ARS: IA-7; NIST 800-53/53A: IA-7; PISP: 4.7.7	**Related Controls:**

ASSESSMENT PROCEDURE: IA-7.1

Assessment Objective

Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).

Assessment Methods And Objects

Examine: Identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing cryptographic module authentication.

Incident Response (IR) – *Operational*

IR-1 – Incident Response Policy and Procedures (High)

Control

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed, documented, and implemented effectively to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-61 and current CMS Procedures.

Guidance

The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

Applicability: All	**References:** ARS: IR-1; FISCAM: TSP-3.4; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1; NIST 800-53/53A: IR-1; PISP: 4.8.1	**Related Controls:**

ASSESSMENT PROCEDURE: IR-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents incident response policy and procedures;
(ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review incident response policy and procedures; and
(iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.
Interview: Organizational personnel with incident response planning and plan implementation responsibilities.

ASSESSMENT PROCEDURE: IR-1.2

Assessment Objective

Determine if:
(i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.
Interview: Organizational personnel with incident response planning and plan implementation responsibilities.

IR-2 – Incident Response Training (High)

Control

All personnel shall be trained in their IR roles and responsibilities with respect to a CMS information system. Personnel shall receive periodic refresher training in IR procedures.

Guidance

Procedures and incident response training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.
(2) Executives must receive training in information security basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.

(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	**References:** ARS: IR-2; IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-2; PISP: 4.8.2	**Related Controls:**

ASSESSMENT PROCEDURE: IR-2.1

Assessment Objective

Determine if:
(i) the organization identifies and documents personnel with incident response roles and responsibilities;
(ii) the organization provides incident response training to personnel with incident response roles and responsibilities;
(iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;
(iv) the organization defines the frequency of refresher incident response training; and
(v) the organization provides refresher incident response training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response training; incident response training material; information system security plan; incident response training records; other relevant documents or records.
Interview: Organizational personnel with incident response training and operational responsibilities.

IR-2(0) – Enhancement (High)

Control

Provide training on incident response roles and responsibilities of personnel every 365 days.

Applicability: All	**References:** ARS: IR-2(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-2; PISP: 4.8.2	**Related Controls:**

ASSESSMENT PROCEDURE: IR-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response training; incident response training material; information system security plan (for organization-defined frequency for refresher incident response training); incident response training records; other relevant documents or records.
Interview: Organizational personnel with incident response training and operational responsibilities.

IR-2(1) – Enhancement (High)

Control

Incorporate simulated events as part of incident response training.

Applicability: All	**References:** ARS: IR-2(1); NIST 800-53/53A: IR-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: IR-2(1).1

Assessment Objective

Determine if the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response training; incident response training material; other relevant documents or records.
Interview: Organizational personnel with incident response training and operational responsibilities.

IR-2(2) – Enhancement (High)

Control

Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

Applicability: All	**References:** ARS: IR-2(2); NIST 800-53/53A: IR-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: IR-2(2).1

Assessment Objective

Determine if the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environment.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response training; incident response training material; automated mechanisms supporting incident response training; other relevant documents or records.(Optional)
Interview: Organizational personnel with incident response training and operational responsibilities.(Optional)
Test: Simulated incident response training events.(Optional)

IR-3 – Incident Response Testing and Exercises (High)

Control

The IR capability for a CMS information system shall be tested periodically using appropriate tests, procedures, automated mechanisms, and exercises to determine the plan's effectiveness. The test results, procedures, and exercises employed to conduct the test shall be documented.

Guidance

NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Applicability: All	**References:** ARS: IR-3; IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-3.1

Assessment Objective

Determine if:
(i) the organization defines incident response tests/exercises;
(ii) the organization defines the frequency of incident response tests/exercises;
(iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency; and
(iv) the organization documents the results of incident response tests/exercises.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan; incident response testing material; incident response test results; other relevant documents or records.

IR-3(0) – Enhancement (High)

Control

Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations.

Applicability: All	**References:** ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of organization-defined tests/exercises and organization-defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant documents or records.

IR-3(1) – Enhancement (High)

Control

Employ automated mechanisms to test / exercise the incident response plan.

Guidance

Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.

Applicability: All	**References:** ARS: IR-3(1); NIST 800-53/53A: IR-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: IR-3(1).1

Assessment Objective

Determine if:
(i) the organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability for the information system; and

(ii) the automated mechanisms supporting incident response testing provide more complete coverage of incident response issues, more realistic test/exercise scenarios, and a greater stress on the incident response capability.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan; incident response testing documentation; automated mechanisms supporting incident response tests/exercises; other relevant documents or records.
Interview: Organizational personnel with incident response testing responsibilities.

IR-4 – Incident Handling (High)

Control

An incident handling capability, which includes preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents, shall be established and maintained. Evidence of computer crimes, computer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learned from on-going incident handling activities shall be incorporated into the IR procedures.

Guidance

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.

Applicability: All	References: ARS: IR-4; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4; PISP: 4.8.4	Related Controls: AU-6, PE-6, SI-2

ASSESSMENT PROCEDURE: IR-4.1

Assessment Objective

Determine if:
(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and
(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling; NIST SP 800-61; other relevant documents or records.
Interview: Organizational personnel with incident handling responsibilities.
Test: Incident handling capability for the organization.

IR-4(1) – Enhancement (High)

Control

Employ automated mechanisms to support the incident handling process.

Applicability: All	References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1)	Related Controls:

ASSESSMENT PROCEDURE: IR-4(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to support the incident handling process.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; other relevant documents or records.
Interview: Organizational personnel with incident handling responsibilities.

IR-4(CMS-1) – Enhancement (High)

Control

Document relevant information related to a security incident according to CMS Information Security Incident Handling and Breach Notification Procedures.

Applicability: All	References: ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	Related Controls:

ASSESSMENT PROCEDURE: IR-4(CMS-1).1

Assessment Objective

Determine if:
(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and
(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if relevant information related to a security incident is documented according to the CMS Information Security Incident Handling and Breach Notification Procedures.

Interview: Organizational personnel with incident response training and operational responsibilities to determine if relevant information related to a security incident is documented according to the CMS Information Security Incident Handling and Breach Notification Procedures.

IR-4(CMS-2) – Enhancement (High)

Control

Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.

Applicability: All	**References:** ARS: IR-4(CMS-2); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-4(CMS-2).1

Assessment Objective

Determine if:
(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and
(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if evidence is preserved through technical means, including secured storage of evidence media and "write" protection of evidence media; sound forensics processes and utilities are used that support legal requirements. A chain of custody for forensic evidence is followed.

Interview: Organizational personnel with incident response training and operational responsibilities to determine if evidence is preserved through technical means, including secured storage of evidence media and "write" protection of evidence media; sound forensics processes and utilities are used that support legal requirements. A chain of custody for forensic evidence is followed.

IR-4(CMS-3) – Enhancement (High)

Control

Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure, including isolation or system disconnect.

Applicability: All	**References:** ARS: IR-4(CMS-3); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-4(CMS-3).1

Assessment Objective

Determine if:
(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and
(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if the identification of vulnerabilities exploited during a security incident and security safeguards are implemented to reduce risk and vulnerability exploit exposure.

Interview: Organizational personnel with incident response training and operational responsibilities to determine if the identification of vulnerabilities exploited during a security incident and security safeguards are implemented to reduce risk and vulnerability exploit exposure.

IR-5 – Incident Monitoring (High)

Control

On-going monitoring of the CMS information system for security events shall be conducted. All events and activities associated with system performance shall be monitored for the identification of resources used by processes and user activity that may indicate security threats resulting from user, software, or hardware activity. All information system security incidents shall be tracked and documented on an on-going basis. All user activities shall be subject to monitoring to verify compliance with this policy and to detect actions that may be in violation of this policy.

Guidance

It is good practice to separate system performance issues from incident tracking. However, unexplained system performance changes can be the result of a security incident occurring or data corruption in transmission within the system. Checksums or cyclic redundancy checks (CRCs) can help during the investigation of these problems. While useful for error detection, CRCs cannot be safely relied upon to fully verify data correctness in the face of deliberate (rather than random) changes.
Remote Procedure Calls (RPCs) can cause performance/incident issues. Note: If an attacker (internal or external person) is able to successfully exploit an RPC vulnerability they could gain complete control over a remote computer. This would give the attacker the ability to take any action on the system that they want. For example, an attacker could change web pages, reformat the hard disk, and / or add new users to the local administrators group.
Performance and incident tracking on an on-going basis can denote trends within the system or network architecture.

Applicability: All	**References:** ARS: IR-5; FISCAM: TAC-4.2; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#2.3; NIST 800-53/53A: IR-5; PISP: 4.8.5	**Related Controls:**

ASSESSMENT PROCEDURE: IR-5.1

Assessment Objective

Determine if the organization tracks and documents information system security incidents on an ongoing basis.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; other relevant documents or records.
Interview: Organizational personnel with incident monitoring responsibilities.
Test: Incident monitoring capability for the organization.

IR-5(1) – Enhancement (High)

Control

Employ automated mechanisms to assist in tracking and analyzing security incidents.

Applicability: All	**References:** ARS: IR-5(1); NIST 800-53/53A: IR-5(1)	**Related Controls:**

ASSESSMENT PROCEDURE: IR-5(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident monitoring; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting incident monitoring; other relevant documents or records.
Interview: Organizational personnel with incident monitoring responsibilities.

IR-6 – Incident Reporting (High)

Control

All IS incidents, or suspected incidents, shall be reported to the CMS IT Service Desk (or equivalent organizational function) as soon as an incident comes to the attention of a user of CMS information or information systems. Events and confirmed security incidents by business partners shall also be reported to the CMS IT Service Desk in accordance with established procedures.

Guidance

The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST SP 800-61 provides guidance on incident reporting.

Applicability: All	**References:** ARS: IR-6; FISCAM: TAC-4.2; NIST 800-53/53A: IR-6; PISP: 4.8.6	**Related Controls:**

ASSESSMENT PROCEDURE: IR-6.1

Assessment Objective

Determine if:
(i) the organization promptly reports incident information to appropriate authorities;
(ii) incident reporting is consistent with NIST SP 800-61;
(iii) the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and
(iv) weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident reporting; NIST SP 800-61; incident reporting records and documentation; other relevant documents or records.
Interview: Organizational personnel with incident reporting responsibilities.
Test: Incident reporting capability for the organization.

IR-6(1) – Enhancement (High)

Control

Employ automated mechanisms to assist in the reporting of security incidents.

Applicability: All	**References:** ARS: IR-6(1); NIST 800-53/53A: IR-6(1)	**Related Controls:**

ASSESSMENT PROCEDURE: IR-6(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; other relevant documents or records.

Interview: Organizational personnel with incident reporting responsibilities.

IR-7 – Incident Response Assistance (High)

Control

A CMS IT Service Desk (or equivalent organizational function) shall be in place and shall play an appropriate role in the organization's IR program. The CMS IT Service Desk shall offer advice to users of a CMS information system. Procedures shall be developed, documented, and implemented effectively to facilitate the incident response by providing central incident support resource for CMS information system users.

Guidance

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

Applicability: All	**References:** ARS: IR-7; NIST 800-53/53A: IR-7; PISP: 4.8.7	**Related Controls:**

ASSESSMENT PROCEDURE: IR-7.1

Assessment Objective

Determine if:

(i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and

(ii) the incident response support resource is an integral part of the organization's incident response capability.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; other relevant documents or records.

Interview: Organizational personnel with incident response assistance and support responsibilities.

IR-7(1) – Enhancement (High)

Control

Employ automated mechanisms to increase the availability of incident response-related information and support.

Applicability: All	**References:** ARS: IR-7(1); NIST 800-53/53A: IR-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: IR-7(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support for incident response support.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; other relevant documents or records.

Interview: Organizational personnel with incident response support and assistance responsibilities and organizational personnel that require incident response support and assistance.

Maintenance (MA) – *Operational*

MA-1 – System Maintenance Policy and Procedures (High)

Control

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

Guidance

The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: MA-1; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-1; PISP: 4.9.1	**Related Controls:**

ASSESSMENT PROCEDURE: MA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents information system maintenance policy and procedures;
(ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review information system maintenance policy and procedures; and
(iv) the organization updates information system maintenance policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.

ASSESSMENT PROCEDURE: MA-1.2

Assessment Objective

Determine if:
(i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.

MA-1(FIS-1) – Enhancement (High)

Control

All system software is current, has current and complete documentation, and is still supported by the vendor.

Applicability: All	**References:** FISCAM: TSS-3.2.5, TSS-3.2.6	**Related Controls:**

ASSESSMENT PROCEDURE: MA-1(FIS-1).1

Assessment Objective

Determine if the organization uses current system software with complete documentation and is vendor supported.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Interview: Management and systems programmers about the currency of system software, and the currency and completeness of software documentation.
Interview: System software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.

MA-2 – Controlled Maintenance (High)

Control

Comprehensive maintenance procedures shall be developed, documented, and implemented effectively to conduct controlled periodic on-site and off-site maintenance of the CMS information

systems and of the physical plant within which these information systems reside. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS-approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly.

Guidance

All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Applicability: All; Optional for SS	**References:** ARS: MA-2; FISCAM: TSC-2.4.1, TSC-2.4.2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-2; PISP: 4.9.2	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2.1

Assessment Objective

Determine if the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-2(1) – Enhancement (High)

Control

Maintain maintenance records for each information system that includes:
(a) Date and time of maintenance,
(b) Name of the individual performing the maintenance, name of escort, if applicable,
(c) Description of the maintenance performed, and
(d) List of equipment removed or replaced (including identification numbers, if applicable).

Applicability: All; Optional for SS	**References:** ARS: MA-2(1); FISCAM: TSC-2.4.3; NIST 800-53/53A: MA-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2(1).1

Assessment Objective

Determine if the organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records.

MA-2(2) – Enhancement (High)

Control

Employ automated mechanisms to ensure that maintenance is scheduled and conducted as required, and that a record of maintenance actions, both needed and complete, is up-to-date, accurate, and readily available.

Applicability: All	**References:** ARS: MA-2(2); NIST 800-53/53A: MA-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to schedule and conduct maintenance as required, and to create accurate, complete, and available records of all maintenance actions, both needed and completed.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; automated mechanisms supporting information system maintenance activities; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

MA-2(FIS-1) – Enhancement (High)		
Control Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.		
Applicability: All; Optional for SS	**References:** FISCAM: TSC-2.4.4	**Related Controls:**
ASSESSMENT PROCEDURE: MA-2(FIS-1).1		
Assessment Objective Determine if the organization accommodates regular and a reasonable amount of unscheduled maintenance in its data processing operations. **Assessment Methods And Objects** **Examine:** Maintenance documentation. **Examine:** Pertinent policies and procedures. **Interview:** Data processing and user management.		
MA-2(FIS-2) – Enhancement (High)		
Control Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users thus allowing for adequate testing. Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.		
Applicability: All	**References:** FISCAM: TSC-2.4.10, TSC-2.4.11	**Related Controls:**
ASSESSMENT PROCEDURE: MA-2(FIS-2).1		
Assessment Objective Determine if: (i) the organization schedules hardware equipment and related software changes such to minimize user impact and maximize resources for adequate testing; and (ii) the organizational advance notification for hardware equipment changes does not cause unexpected interrupted user services. **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Supporting documentation. **Interview:** Senior management, data processing management, and user management.		
MA-2(PII-1) – Enhancement (High)		
Control In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).		
Applicability: All	**References:** HIPAA: 164.310(a)(2)(iv)	**Related Controls:**
ASSESSMENT PROCEDURE: MA-2(PII-1).1		
Assessment Objective Determine if the organization documents repairs and modifications to the facility containing PII. **Assessment Methods And Objects** **Examine:** Facility documentation (such as floor plan and elevation drawings) are updated when repairs and modifications cause changes to the physical components of the facility containing PII. **Interview:** Organizational personnel, with facility management responsibilities, to determine if facility documents reflect security changes caused by repairs and modifications. **Test:** Facility documentation sample to determine if repairs or modifications document physical security implications when the facility is protecting PII.		
MA-3 – Maintenance Tools (High)		
Control The use of system maintenance tools, including diagnostic and test equipment and administration utilities, shall be approved, controlled, and monitored. Approved tools shall be maintained on an on-going basis.		
Guidance The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.		
Applicability: All	**References:** ARS: MA-3; IRS-1075: 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-3; PISP: 4.9.3	**Related Controls:**

ASSESSMENT PROCEDURE: MA-3.1

Assessment Objective

Determine if:
(i) the organization approves, controls, and monitors the use of information system maintenance tools; and
(ii) the organization maintains maintenance tools on an ongoing basis.

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.

MA-3(1) – Enhancement (High)

Control

Inspect all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.

Guidance

Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

Applicability: All	**References:** ARS: MA-3(1); NIST 800-53/53A: MA-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-3(1).1

Assessment Objective

Determine if the organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-3(2) – Enhancement (High)

Control

Check all media containing diagnostic and test programs for malicious code before the media is used in the system.

Applicability: All	**References:** ARS: MA-3(2); NIST 800-53/53A: MA-3(2)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-3(2).1

Assessment Objective

Determine if the organization checks all media containing diagnostic test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-3(3) – Enhancement (High)

Control

Check all maintenance equipment with the capability of retaining information to ensure that no sensitive information is saved on the equipment and that the equipment is appropriately sanitized prior to release. If the equipment cannot be sanitized, the equipment must remain within the facility or be destroyed, unless an exception is specifically authorized.

Applicability: All	**References:** ARS: MA-3(3); NIST 800-53/53A: MA-3(3)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-3(3).1

Assessment Objective

Determine if:
(i) the organization either checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; and
(ii) the organization retains the maintenance equipment within the facility or destroys the equipment if the equipment cannot be sanitized, unless an appropriate organization official explicitly authorizes an exception.

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-3(4) – Enhancement (High)

Control

Employ automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

Applicability: All	**References:** ARS: MA-3(4); NIST 800-53/53A: MA-3(4)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-3(4).1

Assessment Objective

Determine if the organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; automated mechanisms supporting information system maintenance activities; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.(Optional)

Test: Automated mechanisms supporting information system maintenance activities.(Optional)

MA-4 – Remote Maintenance (High)

Control

Remote maintenance of a CMS information system must be approved by the CIO or his/her designated representative. Remote maintenance procedures shall be developed, documented, and implemented effectively to provide additional controls on remotely executed maintenance and diagnostic activities.

The use of remote diagnostic tools shall be described in the SSP for the information system. Maintenance records for all remote maintenance, diagnostic, and service activities shall be maintained and shall be reviewed periodically by appropriate organization officials. All sessions and remote connections shall be terminated after the remote maintenance is completed. If password-based authentication is used during remote maintenance, the passwords shall be changed following each remote maintenance service.

Guidance

Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST SP 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Applicability: All	**References:** ARS: MA-4; FISCAM: TAC-2.1.3; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4; PISP: 4.9.4	**Related Controls:** IA-2, MP-6

ASSESSMENT PROCEDURE: MA-4.1

Assessment Objective

Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-4(1) – Enhancement (High)

Control

Audit all remote maintenance sessions, and ensure that appropriate information security personnel review the maintenance records of the remote sessions.

Applicability: All	**References:** ARS: MA-4(1); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-4(1).1

Assessment Objective

Determine if:
(i) the organization audits all remote maintenance and diagnostic sessions; and
(ii) designated organizational personnel review the maintenance records of remote sessions.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; maintenance records; audit records; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.

MA-4(2) – Enhancement (High)

Control

Document the use of remote diagnostic tools in the SSP.

Applicability: All	**References:** ARS: MA-4(2); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4(2)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-4(2).1

Assessment Objective

Determine if the organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; information system security plan; maintenance records; audit records; other relevant documents or records.

MA-4(3) – Enhancement (High)

Control

Require that remote diagnostic or maintenance service organizations utilize the same level of security as the CMS system being serviced. If the service organization does not use at least the same level of security, maintenance is prohibited unless the component being serviced is removed from the information system and sanitized (with regard to CMS sensitive information) before the service begins. The component is also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system. If the system cannot be sanitized (e.g., due to a system failure), remote maintenance is not permitted.

Applicability: All	**References:** ARS: MA-4(3); NIST 800-53/53A: MA-4(3)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-4(3).1

Assessment Objective

Determine if the organization does not allow remote diagnostic or maintenance services to be performed by a provider that does not implement for its own information system, a level of security at least as high as the level of security implemented on the information system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; service provider contracts and/or service level agreements; maintenance records; audit records; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities; information system maintenance provider.

MA-4(CMS-1) – Enhancement (High)

Control

If remote maintenance is authorized in writing by the CIO or his/her designated representative:
Encrypt and decrypt diagnostic communications; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, terminate all sessions and remote connections. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.

Applicability: All	**References:** ARS: MA-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-4(CMS-1).1

Assessment Objective

Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that remote maintenance is authorized in writing by the CIO or his/her

designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service.

Interview: Organizational personnel with information system maintenance responsibilities to determine that remote maintenance is authorized in writing by the CIO or his/her designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service.

MA-5 – Maintenance Personnel (High)

Control

Maintenance personnel procedures shall be developed, documented, and implemented effectively to control maintenance of CMS information systems. A list of individuals authorized to perform maintenance on the information system shall be maintained.

Guidance

Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Applicability: All	**References:** ARS: MA-5; NIST 800-53/53A: MA-5; PISP: 4.9.5	**Related Controls:**

ASSESSMENT PROCEDURE: MA-5.1

Assessment Objective

Determine if the organization allows only authorized personnel to perform maintenance on the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-5(0) – Enhancement (High)

Control

Only authorized individuals are allowed to perform maintenance. Ensure maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. Supervise maintenance personnel during the performance of maintenance activities when they do not have the needed access authorizations.

Applicability: All	**References:** ARS: MA-5(0); HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: MA-5; PISP: 4.9.5	**Related Controls:**

ASSESSMENT PROCEDURE: MA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-6 – Timely Maintenance (High)

Control

Maintenance services and parts shall be available in a timely manner.

Guidance

It is good practice to determine the priority of each system based on the criticality of the system for continued business operations. Each system should be prioritized and interconnections between each of the enterprise's systems mapped and dataflow diagrams developed.

Next maintenance contracts as well as emergency maintenance considerations will determine needed availability and pre-placement of spare parts.

Applicability: All	**References:** ARS: MA-6; NIST 800-53/53A: MA-6; PISP: 4.9.6	**Related Controls:**

ASSESSMENT PROCEDURE: MA-6.1

Assessment Objective

Determine if:

(i) the organization defines key information system components;

(ii) the organization defines the time period within which support and spare parts must be obtained after a failure; and

(iii) the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-6(0) – Enhancement (High)

Control

Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twenty-four (24) hours of failure.

Applicability: All	**References:** ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6	**Related Controls:**

ASSESSMENT PROCEDURE: MA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts must be obtained after a failure); other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-CMS-1 – Off-site Physical Repair of Systems (High)

Control

Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality.

Guidance

It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approved Change Management baseline.

Storage media control when encrypted may take special considerations.

Applicability: All	**References:** ARS: MA-CMS-1; PISP: 4.9.7	**Related Controls:** AC-19(CMS-1), AC-3, CP-9, SC-12(CMS-1)

ASSESSMENT PROCEDURE: MA-CMS-1.1

Assessment Objective

Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair.

Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.

MA-CMS-1(CMS-0) – Enhancement (High)

Control

Access to system for repair must be by authorized personnel only. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, check security features to verify they are functioning properly.

Applicability: All	**References:** ARS: MA-CMS-1(CMS-0); HIPAA: 164.310(d)(2)(i)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-CMS-1(CMS-0).1

Assessment Objective

Determine if the organization allows only authorized personnel perform maintenance on the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for repair. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, security features are checked to verify they are functioning properly.

Interview: Organizational personnel with information system maintenance responsibilities determine that only authorized personnel are permitted access to system for repair. Storage media must be

removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, security features are checked to verify they are functioning properly.

MA-CMS-2 – On-site Physical Repair of Systems (High)

Control

Controls shall be developed, documented, and implemented effectively to enable on-site physical repair of systems without compromising security functionality or confidentiality.

Guidance

It is good practice to complete a full security review of a system before it is put back into operation when the system has completed repairs. The repaired system should match the approved Change Management baseline.

Storage media control when encrypted may take special considerations.

Applicability: All	**References:** ARS: MA-CMS-2; PISP: 4.9.8	**Related Controls:** AC-19(CMS-1), AC-3, CP-9, SC-12(CMS-1)

ASSESSMENT PROCEDURE: MA-CMS-2.1

Assessment Objective

Determine if the organization effectively develops procedures, documents procedures, and implements on-site repair of systems without compromising security functionality or confidentiality.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for on-site repair.

Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during on-site repair.

MA-CMS-2(CMS-1) – Enhancement (High)

Control

Access to system for repair must be by authorized personnel only.

Applicability: All	**References:** ARS: MA-CMS-2(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-CMS-2(CMS-1).1

Assessment Objective

Determine if the organization allows only authorized personnel perform maintenance on the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel perform maintenance on the information system.

Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel perform maintenance on the information system.

MA-CMS-2(CMS-2) – Enhancement (High)

Control

Physical repair of servers must be within protected environments.

Applicability: All	**References:** ARS: MA-CMS-2(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-CMS-2(CMS-2).1

Assessment Objective

Determine if the organization performs physical repair of servers within protected environments.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine physical repair of servers is performed within protected environments.

Interview: Organizational personnel with information system maintenance responsibilities to determine physical repair of servers is performed within protected environments.

Media Protection (MP) – *Operational*

MP-1 – Media Protection Policy and Procedures (High)

Control

MP controls and procedures shall be developed, documented, and implemented effectively to address media access; media labeling; media transport; media destruction; media sanitization and clearing; media storage; and disposition of media records. The MP procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: MP-1; FISCAM: TAC-3.4; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1; NIST 800-53/53A: MP-1; PISP: 4.10.1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents media protection policy and procedures;
(ii) the organization disseminates media protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review media protection policy and procedures; and
(iv) the organization updates media protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.

ASSESSMENT PROCEDURE: MP-1.2

Assessment Objective

Determine if:
(i) the media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.

MP-1(PII-1) – Enhancement (High)

Control

Semiannual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss.

Applicability: All	**References:** IRS-1075: 3.2#3.2, 3.2#3.3	**Related Controls:**

ASSESSMENT PROCEDURE: MP-1(PII-1).1

Assessment Objective

Determine if:
(i) the organization verifies semiannual inventories of magnetic tapes containing PII.
the organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss.

Assessment Methods And Objects

Examine: Records of semiannual inventories of PII magnetic tapes conducted. If tapes are missing the initiator is notified and a record of the investigation is documented.

MP-2 – Media Access (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media based on the sensitivity of the CMS information. Automated mechanisms shall be implemented to control access to media storage areas and to audit

access attempts and access granted.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Applicability: All	**References:** ARS: MP-2; FISCAM: TAC-3.1.A.6, TAY-4.1.1; HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1; NIST 800-53/53A: MP-2; PISP: 4.10.2	**Related Controls:**

ASSESSMENT PROCEDURE: MP-2.1

Assessment Objective

Determine if the organization restricts access to information system media to authorized users.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records.

Interview: Organizational personnel with information system media protection responsibilities.

MP-2(1) – Enhancement (High)

Control

Employ automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Guidance

This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

Applicability: All	**References:** ARS: MP-2(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.5; IRS-1075: 4.6#1; NIST 800-53/53A: MP-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MP-2(1).1

Assessment Objective

Determine if:

(i) the organization employs automated mechanisms to restrict access to media storage areas; and

(ii) the organization employs automated mechanisms to audit access attempts and access granted.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records.

Test: Automated mechanisms implementing access restrictions to media storage areas.

MP-3 – Media Labeling (High)

Control

Storage media and information system output shall have external labels affixed to indicate the distribution limitations, applicable security classification, and handling caveats of the information. Specific types of media or hardware components may be exempted from the labeling requirement, so long as the exempted items remain within a secure environment. Only the CIO or his/her designated representative shall have the authority to exempt specific types of media or hardware components from the labeling requirement.

Guidance

An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Applicability: All	**References:** ARS: MP-3; IRS-1075: 4.6#1, 5.1#1.2, 5.3#2.1-2, 5.3#3; NIST 800-53/53A: MP-3; PISP: 4.10.3	**Related Controls:**

ASSESSMENT PROCEDURE: MP-3.1

Assessment Objective

Determine if:
(i) the organization defines its protected environment for media labeling requirements;
(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;
(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and
(iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; information system security plan; removable storage media and information system output; other relevant documents or records.

MP-3(CMS-1) – Enhancement (High)

Control

Off-line backup storage media must be marked according to backup rotation schedule for ease of retrieval.

Applicability: All	**References:** ARS: MP-3(CMS-1); IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-3(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines its protected environment for media labeling requirements;
(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;
(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and
(iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine that off-line backup storage media is marked according to backup rotation schedule for ease of retrieval.

Interview: Organizational personnel with information system media protection responsibilities to determine off-line backup storage media is marked according to backup rotation schedule for ease of retrieval.

MP-4 – Media Storage (High)

Control

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper, within controlled areas. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security level of the information ever recorded on it until destroyed or sanitized using CMS-approved procedures.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST SP 800-56 and 800-57 provide guidance on cryptographic key

establishment and cryptographic key management.

Applicability: All	References: ARS: MP-4; FISCAM: TCC-3.2.4, TCC-3.3.1; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1; NIST 800-53/53A: MP-4; PISP: 4.10.4	Related Controls: AC-19, CP-9, CP-9(4), RA-2, SC-7

ASSESSMENT PROCEDURE: MP-4.1

Assessment Objective

Determine if:
(i) the organization defines controlled areas for information system media;
(ii) the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk;
(iii) the organization defines the specific measures used to protect the selected media and information contained on that media;
(iv) the organization physically controls and securely stores information system media within controlled areas; and
(v) the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media; other relevant documents or records.

MP-4(PII-1) – Enhancement (High)

Control

Evaluate employing an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest, consistent with NIST SP 800-66 guidance.

Applicability: All	References: HIPAA: 164.312(a)(2)(iv)	Related Controls: SC-13

ASSESSMENT PROCEDURE: MP-4(PII-1).1

Assessment Objective

Determine if the organization uses approved cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest.

Assessment Methods And Objects

Examine: Cryptographic software licenses used to protect PII at rest. Cryptography software is consistent with NIST SP 800-66 guidance and FIPS 140 approved.
Interview: Organizational staff to determine if FIPS 140 approved cryptographic software/system for PII data at rest protection is being used.

MP-4(PII-2) – Enhancement (High)

Control

If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information.

Applicability: All	References: IRS-1075: 5.3#2.3, 5.3#3	Related Controls:

ASSESSMENT PROCEDURE: MP-4(PII-2).1

Assessment Objective

Determine if the organization protects, in its entirety, personally identifiable information when on magnetic media with other data.

Assessment Methods And Objects

Examine: Magnetic storage of PII is protected to determine, in its entirety, it is controlled as Federal tax information.
Interview: Organizational staff to determine if PII in its entirety is protected as personally identifiable information.

MP-5 – Media Transport (High)

Control

Physical, administrative, and technical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) to authorized personnel based on the sensitivity of the CMS information.

Guidance

Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with

the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Applicability: All	**References:** ARS: MP-5; FISCAM: TAY-4.1.1, TAY-4.1.4; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.6#2, 4.6#4; NIST 800-53/53A: MP-5; PISP: 4.10.5	**Related Controls:** AC-19, CP-9, CP-9(4)

ASSESSMENT PROCEDURE: MP-5.1

Assessment Objective

Determine if:
(i) the organization identifies personnel authorized to transport information system media outside of controlled areas;
(ii) the organization controls information system media during transport outside of controlled areas; and
(iii) the organization restricts the activities associated with transport of information system media to authorized personnel.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records.

MP-5(1) – Enhancement (High)

Control

All sensitive information stored on digital media are protected during transport outside of controlled areas by using cryptography and tamper proof packaging and (a) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier.
If the use of cryptography is not technically feasible or the sensitive information is stored on non-digital media, written management approval (one level below the CIO) must be obtained prior to transport and the information must be (a) hand carried using securable container via authorized personnel, or (b) if shipped, by United States Postal Service (USPS) Certified Mail with return receipt in tamper-proof packaging.
Correspondence pertaining to a single individual may be mailed through regular USPS mail, but should contain only the minimal amount of sensitive information in order to reduce the risk of unauthorized disclosure (e.g., partially masking social security numbers).

Guidance

Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used.

Applicability: All	**References:** ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MP-5(1).1

Assessment Objective

Determine if:
(i) the organization defines security measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas; and
(ii) the organization protects digital and non-digital media during transport outside of controlled areas using the organization-defined security measures.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media transport records; audit records; other relevant documents or records.
Interview: Organizational personnel with information system media transport responsibilities.

MP-5(2) – Enhancement (High)

Control

Activities associated with the transport of sensitive information system media are documented.

Guidance

Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

Applicability: All	**References:** ARS: MP-5(2); IRS-1075: 3.2#3.1, 4.4#2, 4.6#2; NIST 800-53/53A: MP-5(2)	**Related Controls:**

ASSESSMENT PROCEDURE: MP-5(2).1

Assessment Objective

Determine if:

(i) the organization defines a system of records for documenting activities associated with the transport of information system media; and
(ii) the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media transport records; audit records; other relevant documents or records.

MP-5(3) – Enhancement (High)

Control

Employ an identified custodian at all times to transport information system media.

Guidance

Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

Applicability: All	**References:** ARS: MP-5(3); IRS-1075: 4.4#2, 4.6#2; NIST 800-53/53A: MP-5(3)	**Related Controls:**

ASSESSMENT PROCEDURE: MP-5(3).1

Assessment Objective

Determine if the organization employs an identified custodian at all times to transport information system media.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; information system media transport records; audit records; other relevant documents or records.

Interview: Organizational personnel with information system media transport responsibilities.

MP-5(PII-1) – Enhancement (High)

Control

Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.

Applicability: All	**References:** IRS-1075: 4.4#1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-5(PII-1).1

Assessment Objective

Determine if:
(i) the organization protects and controls PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel; and
(ii) the organization uses locked cabinets or sealed packing cartons while PII data is in transit.

Assessment Methods And Objects

Examine: Rosters or list of authorized personnel to protect and control PII media during transit.

Examine: Cabinets or the containers used for protecting PII during transit to determine if there is sufficient fortification to protect PII.

MP-6 – Media Sanitization and Disposal (High)

Control

Formal documented procedures shall be developed and implemented effectively to ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of data residing on storage devices, equipment, and hard copy documents. Media sanitization actions shall be tracked, documented, and verified. Sanitization equipment and procedures shall be tested periodically to ensure proper functionality.

Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmentally approved manner, to facilitate the disposal of media, both electronic and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. Approved equipment removal procedures for CMS information systems and components that have processed or contained CMS information shall be followed. Inventory and disposition records for media, both electronic and paper, shall be produced, stored, updated, and retained.

Guidance

Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Applicability: All	**References:** ARS: MP-6; FISCAM: TAC-3.4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-1075:	**Related Controls:** MA-4

	4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2; NIST 800-53/53A: MP-6; PISP: 4.10.6	

ASSESSMENT PROCEDURE: MP-6.1

Assessment Objective

Determine if:
(i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process;
(ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and
(iii) information system media sanitation is consistent with NIST SP 800-88.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization records; audit records; other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

MP-6(0) – Enhancement (High)

Control

The sanitization process includes the removal of all data, labels, marking, and activity records using NSA Guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, Guidelines for Media Sanitization.

Applicability: All	**References:** ARS: MP-6(0); FISCAM: TAC-3.4; IRS-1075: 8.4#2, 8.4#3; NIST 800-53/53A: MP-6; PISP: 4.10.6	**Related Controls:**

ASSESSMENT PROCEDURE: MP-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization records; audit records; other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

MP-6(CMS-1) – Enhancement (High)

Control

Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.

Applicability: All	**References:** ARS: MP-6(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: MP-6(CMS-1).1

Assessment Objective

Determine if:
(i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process;
(ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and
(iii) information system media sanitation is consistent with NIST SP 800-88.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine hard copy documents are finely shred, using a minimum of cross-cut shredding, using approved equipment, techniques, and procedures.
Interview: Organizational personnel with information system media protection responsibilities to determine hard copy documents are finely shred, using a minimum of cross-cut shredding, using approved equipment, techniques, and procedures.

MP-6(IRS-1) – Enhancement (High)

Control

FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee.

Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	**References:** IRS-1075: 8.4#1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-6(IRS-1).1

Assessment Objective

Determine if:
(i) the organization never discloses FTI to the agency's agents or contractors during disposal unless authorized by the Internal Revenue Code; and
(ii) the organization, generally, uses an agency employee to witness FTI destruction.

Assessment Methods And Objects

Examine: FTI disposal records to determine if unauthorized disclose has been given to contractors or other agency agents.

MP-CMS-1 – Media Related Records (High)

Control

Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.

Guidance

It is good practice for, electronic, inventory records maintenance that a hash function (a reproducible method of turning inventory data into a (relatively) small number that may serve as a digital "fingerprint" of the data) be performed periodically so that the inventory information can be validated as not being tampered with prior to reconstructive events for an investigation of a possible breach.

Applicability: All	References: ARS: MP-CMS-1; FISCAM: TCC-3.2.4; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4; PISP: MP-CMS-1	Related Controls:

ASSESSMENT PROCEDURE: MP-CMS-1.1

Assessment Objective

Determine if the organization maintains inventory and disposition records for information system media to ensure control and accountability of CMS information.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information.

Interview: Organizational personnel with information system media protection responsibilities to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information.

MP-CMS-1(CMS-0) – Enhancement (High)

Control

The media records must, at a minimum, contain:
(a) The name of media recipient;
(b) Signature of media recipient;
(c) Date / time media received;
(d) Media control number and contents;
(e) Movement or routing information; and
(f) If disposed of, the date, time, and method of destruction.

Applicability: All	References: ARS: MP-CMS-1(CMS-0); FISCAM: TCC-3.2.4; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4	Related Controls:

ASSESSMENT PROCEDURE: MP-CMS-1(CMS-0).1

Assessment Objective

Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information. The media records shall contain sufficient information to reconstruct the data in the event of a breach, including but not limited to:
(a) the name of media recipient;
(b) signature of media recipient;
(c) date / time media received;
(d) media control number and contents;
(e) movement or routing information; and
(f) if disposed of, the date, time, and method of destruction.

Interview: Organizational personnel with information system media protection responsibilities to determine inventory and disposition records are maintained for information system media to ensure

control and accountability of CMS information. The media records shall contain sufficient information to reconstruct the data in the event of a breach, including but not limited to:
(a) the name of media recipient;
(b) signature of media recipient;
(c) date / time media received;
(d) media control number and contents;
(e) movement or routing information; and
(f) if disposed of, the date, time, and method of destruction.

MP-CMS-1(PII-1) – Enhancement (High)

Control

For PII, authorized employees of the recipient must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:
• date received
• reel/cartridge control number contents
• number of records, if available
• movement, and
• if disposed of, the date and method of disposition.

Applicability: All	**References:** IRS-1075: 3.2#1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-CMS-1(PII-1).1

Assessment Objective

Determine if:
(i) the organization documents the securing of PII magnetic tapes/cartridges before, during, and after processing, and the proper acknowledgment form is signed and returned; and
(ii) the organizational inventory records maintain PII control and accountability by a log which contains:
• date received
• reel/cartridge control number contents
• number of records, if available
• movement, and
• if disposed of, the date and method of disposition.

Assessment Methods And Objects

Examine: The PII inventory tape/cartridge log for:
• date received
• reel/cartridge control number contents
• number of records, if available
• movement, and
• if disposed of, the date and method of disposition.

MP-CMS-1(IRS-1) – Enhancement (High)

Control

For FTI, organizations are not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7)

Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	**References:** IRS-1075: 11.1#1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-CMS-1(IRS-1).1

Assessment Objective

Determine if the organization allows unauthorized disclosure of FTI data to their agents or to an unauthorized contractor.

Assessment Methods And Objects

Examine: FTI disclosure documentation to determine is authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7)
Interview: Organizational staff to determine if personnel are knowledgeable of IRS Pub. 1075, sect. 11.1 and 11.7 regarding disclosure of FTI data.

Physical and Environmental Protection (PE) – *Operational*

PE-1 – Physical and Environmental Protection Policy and Procedures (High)

Control

Physical and environmental protection procedures shall be developed and implemented effectively to protect all CMS IT infrastructure and assets from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional. These procedures shall meet all federal, state and local building codes and be consistent with General Services Administration policies, directives, regulations, and guidelines.

Guidance

The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: PE-1; FISCAM: TSC-2.2.6, TSC-2.3.4, TSD-2.1; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1; NIST 800-53/53A: PE-1; PISP: 4.11.1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents physical and environmental protection policy and procedures;
(ii) the organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review physical and environmental protection policy and procedures; and
(iv) the organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Physical and environmental protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with physical and environmental protection responsibilities.

ASSESSMENT PROCEDURE: PE-1.2

Assessment Objective

Determine if:
(i) the physical and environmental protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Physical and environmental protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with physical and environmental protection responsibilities.

PE-1(FIS-1) – Enhancement (High)

Control

Eating, drinking, and other behavior that may damage computer equipment is prohibited.

Applicability: All	**References:** FISCAM: TSC-2.2.7	**Related Controls:**

ASSESSMENT PROCEDURE: PE-1(FIS-1).1

Assessment Objective

Determine if the organization prohibits eating, drinking, and other behavior that may damage computer equipment.

Assessment Methods And Objects

Examine: Employee behavior.
Examine: Employee rules of behavior.
Examine: Pertinent policies and procedures.
Interview: Information system management and users.

PE-2 – Physical Access Authorizations (High)

Control

Access lists of personnel with authorized access to facilities containing CMS information or information systems (except for those areas within the facilities officially designated as publicly accessible) shall be documented on standard forms, maintained on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessary, updated. Appropriate authorization credentials (e.g., badges, identification cards, smart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be removed promptly from all access lists.

Guidance

Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides.

Applicability: All	**References:** ARS: PE-2; FISCAM: TAC-2.1.1, TAC-2.1.2, TAC-2.1.4, TAC-2.2, TAC-3.1.A.3, TAC-3.1.A.4, TAC-3.1.A.8, TSS-1.2.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	**Related Controls:**

ASSESSMENT PROCEDURE: PE-2.1

Assessment Objective

Determine if:
(i) the organization identifies areas within the facility that are publicly accessible;
(ii) the organization defines the frequency of review and approval for the physical access list and authorization credentials for the facility;
(iii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
(iv) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and
(v) designated officials within the organization review and approve the access list and authorization credentials at the organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records.

PE-2(0) – Enhancement (High)

Control

Review and approve lists of personnel with authorized access to facilities containing information systems at least once every 90 days.

Applicability: All	**References:** ARS: PE-2(0); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-3.1.A.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	**Related Controls:**

ASSESSMENT PROCEDURE: PE-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records.

PE-2(PII-1) – Enhancement (High)

Control

Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.

Applicability: All	**References:** IRS-1075: 4.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-2(PII-1).1

Assessment Objective

Determine if:
(i) the organization created a restricted area, security room, or locked room to control access to areas containing PII; and
(ii) the organization controls a restricted area, security room, or locked room in accordance with BPSSM.

Assessment Methods And Objects

Examine: Restricted areas, security rooms, or locked rooms that control access to areas containing PII to determine if control and fortification functions are in accordance with BPSSM.
Interview: Facility personnel responsible for controlling restricted areas, security rooms, or locked rooms containing PII to determine compliance with BPSSM.

PE-3 – Physical Access Control (High)

Control

Physical access control devices (e.g., keys, locks, combinations, card-readers) and/or guards shall be used to control entry to and exit from facilities containing CMS information or information systems, except for areas and/or facilities officially designated as publicly accessible. Individual access authorizations shall be verified before granting access to facilities containing CMS information or information systems. Physical access control devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis.

Combinations, access codes, and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry to facilities during emergency-related events shall be restricted to authorized individuals only. Access to workstations and associated peripheral computing devices shall be appropriately controlled when located in areas designated as publicly accessible.

Guidance

The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST SP 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST SP 800-76.

Applicability: All	**References:** ARS: PE-3; FISCAM: TAC-3.1.A.3, TAC-3.1.A.5, TAC-3.1.A.7, TAC-3.1.A.8, TAC-3.1.B.2, TAN-2.1.1, TAN-2.1.2, TAN-2.2.1, TSD-2.1; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1; NIST 800-53/53A: PE-3; PISP: 4.11.3	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3.1

Assessment Objective

Determine if:
(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
(ii) the organization verifies individual access authorizations before granting access to the facility; and
(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records.
Interview: Organizational personnel with physical access control responsibilities.
Test: Physical access control capability.

ASSESSMENT PROCEDURE: PE-3.2

Assessment Objective

Determine if:
(i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis;
(ii) the organization secures keys, combinations and other access devices on a regular basis; and
(iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records.
Test: Physical access control devices.

ASSESSMENT PROCEDURE: PE-3.3

Assessment Objective

Determine if:
(i) the access control system is consistent with FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed);
(ii) the access control system is consistent with NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and
(iii) the access control system is consistent with NIST SP 800-76 (where the token-based access control function employs biometric verification).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST SP 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records.

Test: Physical access control devices.

PE-3(1) – Enhancement (High)

Control

Physical access control to the information system is independent of the physical access controls for the facility.

Guidance

This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.

Applicability: All	**References:** ARS: PE-3(1); IRS-1075: 4.6#1; NIST 800-53/53A: PE-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(1).1

Assessment Objective

Determine if:

(i) the organization identifies specific areas within the facility containing large concentrations of information system components or components requiring additional physical protection; and

(ii) for an information system identified as requiring additional physical protection or part of a large concentration of information system components, the organization controls physical access to the system independent of the physical access controls for the facility.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; other relevant documents or records.

PE-3(CMS-1) – Enhancement (High)

Control

Control data center / facility access by use of door and window locks, and security staff or physical authentication devices, such as biometrics and/or smart card / PIN combination.

Applicability: All	**References:** ARS: PE-3(CMS-1); IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-1).1

Assessment Objective

Determine if the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine data center / facility access is controlled by use of door and window locks.

Interview: Organizational personnel with physical access control responsibilities to confirm data center / facility access is controlled by use of door and window locks.

Test: Physical access control capability to determine data center / facility access is controlled by use of door and window locks.

PE-3(CMS-2) – Enhancement (High)

Control

Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.

Applicability: All	**References:** ARS: PE-3(CMS-2); FISCAM: TAC-3.1.A.5; IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-2).1

Assessment Objective

Determine if the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine servers are stored and operated in physically secure environments protected from unauthorized access.

Interview: Organizational personnel with physical access control responsibilities to determine servers are stored and operated in physically secure environments protected from unauthorized access.

Test: Physical access to Data Center to determine servers are stored and operated in physically secure environments protected from unauthorized access.

PE-3(CMS-3) – Enhancement (High)

Control

Data centers must meet the minimum requirements as established by the Federal Information Systems Control Audit Manual (FISCAM).

Applicability: All	**References:** ARS: PE-3(CMS-3); FISCAM: TAC-3.1.A.1, TAN-2.1.1, TAN-2.1.2; IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-3).1

Assessment Objective

Determine if:
(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
(ii) the organization verifies individual access authorizations before granting access to the facility; and
(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if data centers meet the minimum requirements as established by the Federal Information Systems Control Audit Manual (FISCAM).

PE-3(CMS-4) – Enhancement (High)

Control

Restrict access to grounds / facilities to authorized persons only.

Applicability: All	**References:** ARS: PE-3(CMS-4); IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-4).1

Assessment Objective

Determine if the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if access to grounds / facilities is restricted to authorized persons only.
Interview: Organizational personnel with physical access control responsibilities to determine access to grounds / facilities is restricted to authorized persons only.
Test: Physical access controls to determine if access to grounds / facilities is restricted to authorized persons only.

PE-3(PII-1) – Enhancement (High)

Control

For PII, require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access after hours.

Applicability: All	**References:** IRS-1075: 4.2#2	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(PII-1).1

Assessment Objective

Determine if:
(i) the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; and
(ii) the organization containerizes protected information in areas where other than authorized employees may have access after hours.

Assessment Methods And Objects

Examine: Barriers to protect PII to determine two (2) barriers are present for normal security.
Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours.
Interview: Organizational personnel to determine if PII has been disclosed to unauthorized employees.
Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel.

PE-3(DIR-1) – Enhancement (High)

Control

Controls are established to protect access authorization lists to secure areas such as data centers.

Applicability: All	**References:**	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(DIR-1).1

Assessment Objective

Determine if the organization protects approved access authorization lists that are for secure areas.

Assessment Methods And Objects

Examine: Protection procedures are in place for approved access authorization lists to secure areas.

PE-4 – Access Control for Transmission Medium (High)

Control

Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering of CMS information system transmission lines within organizational facilities that carry unencrypted information.

Guidance

Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Applicability: All	**References:** ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4	**Related Controls:**

ASSESSMENT PROCEDURE: PE-4.1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records.

PE-4(CMS-1) – Enhancement (High)

Control

Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel.

Applicability: All	**References:** ARS: PE-4(CMS-1); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-4(CMS-1).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

Interview: Organizational personnel with physical access control responsibilities to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

Test: Physical access controls to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

PE-4(CMS-2) – Enhancement (High)

Control

Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use.

Applicability: All	**References:** ARS: PE-4(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-4(CMS-2).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

Interview: Organizational personnel with physical access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

Test: Physical access controls to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

PE-5 – Access Control for Display Medium (High)

Control

Physical access controls shall be developed, documented, and implemented effectively to prevent unauthorized individuals from observing CMS sensitive information displayed on information system devices.

Guidance

It is good practice to position sensitive information display devices away from windows and areas of ingress and egress.

Applicability: All	References: ARS: PE-5; FISCAM: TAN-2.1.1; HIPAA: 164.310(b); NIST 800-53/53A: PE-5; PISP: 4.11.5	Related Controls:

ASSESSMENT PROCEDURE: PE-5.1

Assessment Objective

Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; other relevant documents or records.

PE-6 – Monitoring Physical Access (High)

Control

Physical access to information systems shall be monitored for physical security compliance and to detect and respond to incidents. Appropriate organization officials shall periodically review physical access records, investigate apparent security violations or suspicious physical access activities, and take appropriate remedial action.

Guidance

The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.

Applicability: All	References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN-2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6	Related Controls: IR-4

ASSESSMENT PROCEDURE: PE-6.1

Assessment Objective

Determine if the organization monitors physical access to the information system to detect and respond to physical security incidents.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; other relevant documents or records.
Interview: Organizational personnel with physical access monitoring responsibilities.
Test: Physical access monitoring capability.

PE-6(1) – Enhancement (High)

Control

Monitor real-time physical intrusion alarms and surveillance equipment.

Applicability: All	References: ARS: PE-6(1); NIST 800-53/53A: PE-6(1)	Related Controls:

ASSESSMENT PROCEDURE: PE-6(1).1

Assessment Objective

Determine if the organization monitors real-time intrusion alarms and surveillance equipment.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; intrusion alarm/surveillance equipment logs or records; other relevant documents or records.
Interview: Organizational personnel with physical access monitoring responsibilities.

PE-6(2) – Enhancement (High)

Control

Automated mechanisms are implemented to recognize potential intrusions and initiate appropriate response actions.

Applicability: All	References: ARS: PE-6(2); NIST 800-53/53A: PE-6(2)	Related Controls:

ASSESSMENT PROCEDURE: PE-6(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; information system design documentation; other relevant documents or records.

Test: Automated mechanisms implementing physical access monitoring capability.

PE-7 – Visitor Control (High)

Control

Visitor controls shall be developed, documented, and implemented effectively to control access to sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries. Visitors shall be authenticated prior to being granted access to facilities or areas other than areas designated as publicly accessible. Government contractors and others with permanent authorization credentials are not considered visitors.

Guidance

Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST SP 800-79.

Applicability: All	**References:** ARS: PE-7; FISCAM: TAC-3.1.B.3; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7; PISP: 4.11.7	**Related Controls:**

ASSESSMENT PROCEDURE: PE-7.1

Assessment Objective

Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.

Interview: Organizational personnel with visitor access control responsibilities.

Test: Visitor access control capability.

PE-7(1) – Enhancement (High)

Control

Escort visitors and monitor visitor activity.

Applicability: All	**References:** ARS: PE-7(1); FISCAM: TAC-3.1.B.1; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-7(1).1

Assessment Objective

Determine if the organization escorts visitors and monitors visitor activity, when required.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.

Interview: Organizational personnel with visitor access control responsibilities.

PE-7(FIS-1) – Enhancement (High)

Control

Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.

Applicability: All	**References:** FISCAM: TAC-3.1.B.3	**Related Controls:**

ASSESSMENT PROCEDURE: PE-7(FIS-1).1

Assessment Objective

Determine if the organization authenticates visitors, contractors and maintenance personnel through the use of preplanned appointments and identification checks.

Assessment Methods And Objects

Examine: Appointment and verification procedures for visitors.

Examine: Pertinent policies and procedures.

Interview: Receptionist or security guard.

PE-8 – Access Records (High)

Control

Visitor access to sensitive facilities and restricted / controlled areas that contain CMS information or information systems shall be logged. The visitor access record shall contain:
4.11.8.1. Name and organization of the person visiting;
4.11.8.2. Signature of the visitor;
4.11.8.3. Form of identification;
4.11.8.4. Date of access;
4.11.8.5. Time of entry and departure;
4.11.8.6. Purpose of visit; and
4.11.8.7. Name and organization of person visited.

Appropriate organization officials shall periodically review the access records, including after closeout.

Guidance

It is good practice to have a standard log format for consistency and ease of use during log closeouts and the next months log generation.

Applicability: All	**References:** ARS: PE-8; FISCAM: TAC-3.1.B.1, TAC-3.1.B.3; NIST 800-53/53A: PE-8; PISP: 4.11.8	**Related Controls:**

ASSESSMENT PROCEDURE: PE-8.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of review for visitor access records;
(ii) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes:
- name and organization of the person visiting;
- signature of the visitor;
- form of identification;
- date of access;
- time of entry and departure;
- purpose of visit;
- name and organization of person visited and

(iii) designated officials within the organization review the visitor access logs in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan; facility access control records; other relevant documents or records.

PE-8(0) – Enhancement (High)

Control

Visitor access records must be closed out and reviewed by management monthly.

Applicability: All	**References:** ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8	**Related Controls:**

ASSESSMENT PROCEDURE: PE-8(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan (for organization-defined frequency for review of visitor access records); facility access control records; other relevant documents or records.

PE-8(1) – Enhancement (High)

Control

Employ automated mechanisms to facilitate the maintenance and review of access records.

Applicability: All	**References:** ARS: PE-8(1); NIST 800-53/53A: PE-8(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-8(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to facilitate the maintenance and review of access records.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; automated mechanisms supporting management of access records; facility access control logs or records; other relevant documents or records.

PE-8(2) – Enhancement (High)

Control

Maintain records of all physical access, both visitor and authorized individuals.

Applicability: All	**References:** ARS: PE-8(2); NIST 800-53/53A: PE-8(2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-8(2).1

Assessment Objective

Determine if the organization maintains a record of all physical access, both visitor and authorized individuals.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; facility access control logs or records; other relevant documents or records.

PE-9 – Power Equipment and Power Cabling (High)

Control

Power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain safe power for CMS information systems.

Guidance

Both primary and backup power systems should be included in the safe power implementation procedures. Remote backup site's power implementation should be included in the documentation.

Applicability: All	**References:** ARS: PE-9; NIST 800-53/53A: PE-9; PISP: 4.11.9	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9.1

Assessment Objective

Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.

PE-9(1) – Enhancement (High)

Control

Employ redundant and parallel power cabling paths.

Applicability: All	**References:** ARS: PE-9(1); NIST 800-53/53A: PE-9(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9(1).1

Assessment Objective

Determine if the organization employs redundant and parallel power cabling paths.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.(Optional)

PE-9(CMS-1) – Enhancement (High)

Control

Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

Applicability: All	**References:** ARS: PE-9(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9(CMS-1).1

Assessment Objective

Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

Interview: Organizational personnel with physical access control responsibilities to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

PE-9(CMS-2) – Enhancement (High)

Control

Power surge protection must be implemented for all computer equipment.

Applicability: All	**References:** ARS: PE-9(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9(CMS-2).1

Assessment Objective

Determine if the organization protects power equipment and implements surge protection for all computers to assist in protection from damage or destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents /records / diagrams to determine if power surge protection is implemented for all computer equipment.

Interview: Organizational personnel with physical access control responsibilities to determine if power surge protection is implemented for all computer equipment.

Test: Verify by physical inspection to determine if power surge protection is implemented for all computer equipment.

PE-10 – Emergency Shutoff (High)

Control

Emergency shut-off controls shall be developed, documented, and implemented effectively to provide the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

Guidance

Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Applicability: All	**References:** ARS: PE-10; NIST 800-53/53A: PE-10; PISP: 4.11.10	**Related Controls:**

ASSESSMENT PROCEDURE: PE-10.1

Assessment Objective

Determine if:

(i) the organization defines the specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms); and

(ii) the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records.

PE-10(1) – Enhancement (High)

Control

Employ appropriate measures to protect the emergency power-off capability from accidental and intentional / unauthorized activation.

Applicability: All	**References:** ARS: PE-10(1); NIST 800-53/53A: PE-10(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-10(1).1

Assessment Objective

Determine if the organization protects the emergency power-off capability from accidental or unauthorized activation.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records.

PE-10(CMS-1) – Enhancement (High)

Control

Implement and maintain a master power switch or emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms.

Applicability: All	**References:** ARS: PE-10(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-10(CMS-1).1

Assessment Objective

Determine if the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms.

Interview: Organizational personnel with physical access control responsibilities to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms.

Test: Verify by physical inspection to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms.

PE-11 – Emergency Power (High)

Control

Emergency power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to facilitate an orderly shutdown of the CMS information system in the event of a primary power source loss.

Guidance

Both primary and backup processing locations should be included in the safe power implementation procedures. The remote backup site's power implementation should be included in the documentation. Even though unlikely that both the primary and backup locations will be switching to emergency power at the same time, it is prudent to minimize the risk to a total lose of a processing capability.

Applicability: All	**References:** ARS: PE-11; FISCAM: TSC-2.2.5; NIST 800-53/53A: PE-11; PISP: 4.11.11	**Related Controls:**

ASSESSMENT PROCEDURE: PE-11.1

Assessment Objective

Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records.

Test: Uninterruptible power supply.

PE-11(1) – Enhancement (High)

Control

Provide a long-term alternate power supply for the system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Applicability: All	**References:** ARS: PE-11(1); NIST 800-53/53A: PE-11(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-11(1).1

Assessment Objective

Determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records.

Test: Alternate power supply.

PE-12 – Emergency Lighting (High)

Control

Mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enhance safety and availability. Automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes shall be provided.

Guidance

Local building safety codes are a good place to obtain the needed information for documenting emergency lighting implementation procedures and architecture.

Applicability: All	**References:** ARS: PE-12; NIST 800-53/53A: PE-12; PISP: 4.11.12	**Related Controls:**

ASSESSMENT PROCEDURE: PE-12.1

Assessment Objective

Determine if:
(i) the organization employs and maintains automatic emergency lighting systems that activates in the event of a power outage or disruption; and
(ii) the organization employs and maintains automatic emergency lighting systems that cover emergency exits and evacuation routes.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records.
Test: Emergency lighting capability.

PE-13 – Fire Protection (High)

Control

Fire protection mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to prevent, detect, and respond to fire. Fire suppression and detection devices / systems that can be activated in the event of a fire shall be employed and maintained. Fire suppression and detection devices / systems shall include, but not be limited to, sprinkler systems, hand-held fire extinguishers, fixed fire hoses, and smoke detectors.

Guidance

Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Applicability: All	**References:** ARS: PE-13; FISCAM: TSC-2.2.1, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-13; PISP: 4.11.13	**Related Controls:**

ASSESSMENT PROCEDURE: PE-13.1

Assessment Objective

Determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records.

PE-13(1) – Enhancement (High)

Control

Implement and maintain fire detection devices / systems that activate automatically and notify the organization and emergency responders in the event of a fire.

Applicability: All	**References:** ARS: PE-13(1); NIST 800-53/53A: PE-13(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-13(1).1

Assessment Objective

Determine if:
(i) the organization employs fire detection devices/systems that activate automatically; and
(ii) the organization employs fire detection devices/systems that notify the organization and emergency responders in the event of a fire.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; other relevant documents or records.
Test: Simulated fire detection and automated notifications.

PE-13(2) – Enhancement (High)

Control

Employ fire suppression devices / systems that provide automatic notification of any activation to the organization and emergency responders.

Applicability: All	**References:** ARS: PE-13(2); NIST 800-53/53A: PE-13(2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-13(2).1

Assessment Objective

Determine if the organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system;

alarm service level agreements; test records of fire suppression and detection devices/systems; other relevant documents or records.
Test: Simulated activation of fire suppression devices/systems and automated notifications.

PE-13(3) – Enhancement (High)

Control

Employ an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

Applicability: All	**References:** ARS: PE-13(3); NIST 800-53/53A: PE-13(3)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-13(3).1

Assessment Objective

Determine if the organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; other relevant documents or records.
Test: Simulated activation of fire suppression devices/systems and automated notifications.

PE-14 – Temperature and Humidity Controls (High)

Control

Temperature and humidity control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain (within acceptable levels) and monitor the temperature and humidity of facilities containing CMS information systems.

Guidance

Local building a safety codes are a good place to obtain the needed information for documenting HVAC implementation procedures and architecture. Consideration for Occupational Safety and Health Administration (OSHA) requirements maybe included.

Applicability: All	**References:** ARS: PE-14; FISCAM: TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-14; PISP: 4.11.14	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14.1

Assessment Objective

Determine if:
(i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and
(ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records.

PE-14(CMS-1) – Enhancement (High)

Control

Evaluate the level of alert and follow prescribed guidelines for that alert level.

Applicability: All	**References:** ARS: PE-14(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(CMS-1).1

Assessment Objective

Determine if:
(i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and
(ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records to determine the level of alert and prescribed guidelines for that alert level.
Interview: Organizational personnel with environmental protection responsibilities to determine if there exists the level of alert and prescribed guidelines for that alert level.

PE-14(CMS-2) – Enhancement (High)

Control

Alert component management of possible loss of service and/or media.

Applicability: All	**References:** ARS: PE-14(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(CMS-2).1

Assessment Objective

Determine if the organization alerts responsible management personnel of loss of service or media.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records to determine an alert is generated to component management of possible loss of service and/or media.

Interview: Organizational personnel with environmental protection responsibilities to determine an alert is generated to component management of possible loss of service and/or media.

PE-14(CMS-3) – Enhancement (High)

Control

Report damage and provide remedial action. Implement contingency plan, if necessary.

Applicability: All	**References:** ARS: PE-14(CMS-3)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(CMS-3).1

Assessment Objective

Determine if the organization regularly monitors the temperature and humidity within the facility where the information system resides.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records to determine damage is reported and remedial action is taken, including the implementation of contingency plan.

Interview: Organizational personnel with environmental protection responsibilities to determine to determine if damage is reported and remedial action is taken, including the implementation of contingency plan.

PE-14(FIS-1) – Enhancement (High)

Control

Redundancy exists in the air cooling system.

Applicability: All	**References:** FISCAM: TSC-2.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(FIS-1).1

Assessment Objective

Determine if the organization uses redundant air cooling systems.

Assessment Methods And Objects

Examine: Entity's facilities.

Examine: Operation, location, maintenance, and access to the air cooling systems.

Examine: Pertinent policies and procedures.

Interview: Site manager.

PE-15 – Water Damage Protection (High)

Control

All necessary steps shall be taken to ensure that the building plumbing does not endanger CMS information systems. Procedures shall be developed, documented, and implemented effectively to reduce the potential damage from plumbing leaks.

Guidance

Local building a safety codes are a good place to obtain the needed information for documenting water damage protection procedures and architecture. Consideration for Occupational Safety and Health Administration (OSHA) requirements maybe included.

Applicability: All	**References:** ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15; PISP: 4.11.15	**Related Controls:**

ASSESSMENT PROCEDURE: PE-15.1

Assessment Objective

Determine if:

(i) the organization identifies key personnel with knowledge of location and operational procedures for activating master shutoff valves for plumbing system; and

(ii) the organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff values; list of key personnel with knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value documentation; other relevant documents or records.
Interview: Organization personnel with physical and environmental protection responsibilities.
Test: Simulated master water shutoff value activation for the plumbing system.

PE-15(1) – Enhancement (High)

Control

Mechanisms are employed that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.

Applicability: All	**References:** ARS: PE-15(1); NIST 800-53/53A: PE-15(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-15(1).1

Assessment Objective

Determine if the organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; automated mechanisms for water shutoff valves; other relevant documents or records.
Test: Automated mechanisms implementing master water shutoff valve activation.

PE-16 – Delivery and Removal (High)

Control

Procedures shall be developed, documented, and implemented effectively to control the flow of information system-related items into and out of the organization. Appropriate officials shall authorize the delivery or removal of CMS information system-related items.

To avoid unauthorized access, delivery and removal controls shall be implemented to isolate delivery areas from sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries.

Guidance

The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.

Applicability: All	**References:** ARS: PE-16; NIST 800-53/53A: PE-16; PISP: 4.11.16	**Related Controls:**

ASSESSMENT PROCEDURE: PE-16.1

Assessment Objective

Determine if:
(i) the organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility; and
(ii) the organization maintains appropriate records of items entering and exiting the facility.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records.
Interview: Organization personnel with tracking responsibilities for information system components entering and exiting the facility.

PE-17 – Alternate Work Site (High)

Control

Procedures shall be developed, documented, and implemented effectively to control information system security at alternate work sites. A method of communication shall be provided to employees at alternate work sites to report security issues or suspected security incidents.

Guidance

The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST SP 800-46 provides guidance on security in telecommuting and broadband communications.

Applicability: All	**References:** ARS: PE-17; HIPAA: 164.310(a)(2)(i); NIST 800-53/53A: PE-17; PISP: 4.11.17	**Related Controls:**

ASSESSMENT PROCEDURE: PE-17.1

Assessment Objective

Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records.

Interview: Organization personnel using alternate work sites.

PE-17(CMS-1) – Enhancement (High)

Control

Employ appropriate security controls at alternate work sites. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

Applicability: All	**References:** ARS: PE-17(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-17(CMS-1).1

Assessment Objective

Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records to determine if appropriate security controls at alternate work sites are employed. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

Interview: Organizational personnel with alternate worksite responsibilities to determine if appropriate security controls at alternate work sites are employed. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

PE-18 – Location of Information System Components (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that information system components are positioned within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.

Guidance

Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Applicability: All	**References:** ARS: PE-18; FISCAM: TAN-2.1.1, TAN-2.1.2; HIPAA: 164.312(c)(1); NIST 800-53/53A: PE-18; PISP: 4.11.18	**Related Controls:**

ASSESSMENT PROCEDURE: PE-18.1

Assessment Objective

Determine if:

(i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and

(ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; other relevant documents or records.

PE-18(1) – Enhancement (High)

Control

Plan the location or site of information system facilities with regard to physical and environmental hazards and, for existing facilities, consider the physical and environmental hazards in the risk mitigation strategy.

Applicability: All	**References:** ARS: PE-18(1); NIST 800-53/53A: PE-18(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-18(1).1

Assessment Objective

Determine if:

(i) the organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards; and

(ii) the organization, for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; physical site planning documents; organizational assessment of risk, contingency plan; other relevant documents or records.
Interview: Organization personnel with site selection responsibilities for the facility housing the information system.

PE-19 – Information Leakage (Optional) (High)

Control

Safeguards and countermeasures should be considered to protect information systems against information leakage due to electromagnetic signals emanations.

Guidance

The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Applicability: Optional for all	**References:** ARS: PE-19; NIST 800-53/53A: PE-19; PISP: 4.11.19	**Related Controls:**

ASSESSMENT PROCEDURE: PE-19.1

Assessment Objective

Determine if the organization protects the information system from information leakage due to electromagnetic signals emanations.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing information leakage due to electromagnetic signals emanations; mechanisms protecting the information system against electronic signals emanation; facility housing the information system; records from electromagnetic signals emanation tests; other relevant documents or records.(Optional)
Test: Information system for information leakage due to electromagnetic signals emanations.(Optional)

Planning (PL) – *Management*

PL-1 – Security Planning Policy and Procedures (High)

Control

All CMS information systems and major applications shall be documented in a SSP, which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, in accordance with current CMS Procedures.

Guidance

The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-18 provides guidance on security planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: PL-1; FISCAM: TSP-2.1, TSP-3.2; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2; NIST 800-53/53A: PL-1; PISP: 4.12.1	**Related Controls:**

ASSESSMENT PROCEDURE: PL-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security planning policy and procedures;
(ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review security planning policy and procedures; and
(iv) the organization updates security planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.

ASSESSMENT PROCEDURE: PL-1.2

Assessment Objective

Determine if:
(i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.

PL-1(FIS-1) – Enhancement (High)

Control

Security policies are distributed to all affected personnel.

Applicability: All	**References:** FISCAM: TSP-3.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-1(FIS-1).1

Assessment Objective

Determine if the organization distributes security policies to all affected personnel.

Assessment Methods And Objects

Examine: Memos, electronic mail files, or other policy distribution mechanisms.
Interview: Staff and system users to determine how security policies are distributed.

PL-2 – System Security Plan (SSP) (High)

Control

All CMS information systems and major applications shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18. The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization

officials and incorporated into the information resources management strategic plan. The information contained in the SSP is subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The security plan is aligned with the organization's information system architecture and information security architecture. NIST SP 800-18 provides guidance on security planning.

Applicability: All	**References:** ARS: PL-2; FISCAM: TAC-3.1.A.1, TSP-2.1, TSP-3.2; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3; NIST 800-53/53A: PL-2; PISP: 4.12.2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2.1

Assessment Objective

Determine if:
(i) the organization develops and implements a security plan for the information system;
(ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements;
(iii) the security plan development is consistent with NIST SP 800-18 and the concepts in the NIST Risk Management Framework including baseline security control selection, tailoring of the baseline, and supplementation of the tailored baseline;
(iv) the security plan is consistent with the organization's information system architecture and information security architecture; and
(v) designated organizational officials review and approve the security plan.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan development and implementation; NIST SP 800-18; security plan for the information system; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.

PL-2(CMS-1) – Enhancement (High)

Control

Document the in-place security controls of the system according to the CMS System Security Plan (SSP) Procedures.

Applicability: All	**References:** ARS: PL-2(CMS-1); FISCAM: TSP-2.1; HIPAA: 164.316(b)(1)(i), 164.316(b)(1)(ii); HSPD 7: J(35); IRS-1075: 4.7.3#2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2(CMS-1).1

Assessment Objective

Determine if:
(i) the organization develops and implements a security plan for the information system;
(ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements;
(iii) the security plan is consistent with NIST SP 800-18;
(iv) the security plan is consistent with the organization's information system architecture and information security architecture; and
(v) designated organizational officials review and approve the security plan.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan development and implementation; NIST SP 800-18; security plan for the information system; other relevant documents or records to determine the in-place security controls of the system are documented according to the CMS System Security Plan (SSP) Procedures.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities to determine if System Security Plan (SSP) includes the in-place security controls of the system and are documented according to the CMS System Security Plan (SSP) Procedures.

PL-2(PII-1) – Enhancement (High)

Control

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Applicability: All	**References:** HIPAA: 164.316(b)(2)(ii)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2(PII-1).1

Assessment Objective

Determine if the organization provides to those persons responsible for implementing the procedures to which the documentation pertains.

Assessment Methods And Objects

Examine: Procedures that document who obtains documentation and which documentation pertains to whom for implementation.
Interview: Organizational personnel who are responsible for implementation of procedures to determine if documentation is available.

PL-2(HIP-1) – Enhancement (High)		
Control Retain documentation of policies and procedures relating to HIPAA 164.306 for 6 years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)		
Applicability: All	**References:** HIPAA: 164.316(b)(2)(i)	**Related Controls:**
ASSESSMENT PROCEDURE: PL-2(HIP-1).1		
Assessment Objective Determine if the organization retains documentation of policies and procedures relating to 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b)) **Assessment Methods And Objects** **Examine:** A sampling of documentation of policies and procedures relating to 164.306 is held for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b)) **Interview:** Organization personnel to determine if documentation of policies and procedures relating to 164.306 is held for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b))		
PL-2(IRS-1) – Enhancement (High)		
Control When FTI is incorporated into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition to those specified in other controls.		
Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	**References:** IRS-1075: 5.6.3.5#3	**Related Controls:**
ASSESSMENT PROCEDURE: PL-2(IRS-1).1		
Assessment Objective Determine if the organization incorporates FTI into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition to those specified in other controls. **Assessment Methods And Objects** **Examine:** Controls to determine compliance with IRS Pub 1075 Exhibit 7 while FTI is incorporated into a Data Warehouse.		
PL-2(IRS-2) – Enhancement (High)		
Control For FTI, develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7 & 8)		
Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	**References:** IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1	**Related Controls:**
ASSESSMENT PROCEDURE: PL-2(IRS-2).1		
Assessment Objective Determine if the organization develops and submits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7 & 8). **Assessment Methods And Objects** **Examine:** Safeguard Procedure Reports to determine the procedures established and used ensure confidentially of the FTI data received from the IRS. **Examine:** Safeguard Activity Reports to determine annual submission and protections are in accordance with the Safeguard Procedure Report.		
PL-3 – System Security Plan Update (High)		
Control The SSP shall be reviewed at least every 365 days and updated minimally every three (3) years to reflect current conditions or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security; when the data sensitivity level increases; after a serious security violation; due to changes in the threat environment; or before the previous accreditation expires.		

Guidance

Significant changes are defined in advance by the organization and identified in the configuration management process. NIST SP 800-18 provides guidance on security plan updates.

Applicability: All	**References:** ARS: PL-3; FISCAM: TSP-2.2; HIPAA: 164.306(a)(3), 164.316(a), 164.316(b)(2)(iii); HSPD 7: G(24), J(35); IRS-1075: 5.6.1.2#1.4; NIST 800-53/53A: PL-3; PISP: 4.12.3	**Related Controls:**

ASSESSMENT PROCEDURE: PL-3.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of information system security plan reviews and updates;
(ii) the organization updates the security plan in accordance with organization-defined frequency, at least annually;
(iii) the organization receives input to update the security plan from the organization's configuration management and control process; and
(iv) the updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan updates; information system security plan; configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records.

PL-4 – Rules of Behavior (ROB) (High)

Control

ROBs shall be established, and made readily available, to delineate clearly user responsibilities and expected behavior of all Business Owners, users, operators, and administrators with regard to information and information system usage. Before authorizing access to the information system and / or information and annually thereafter, the organization shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the ROBs. Specific ROBs shall be established to govern work-at-home users who access CMS information or information systems.

Limited personal use of organization-owned or leased equipment and resources shall be considered to be a permitted use of organization-owned or leased equipment and resources when the following conditions are met:
4.12.4.1. Such use involves minimal additional expense to CMS;
4.12.4.2. Such use does not interfere with the mission or operation of CMS;
4.12.4.3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch;
4.12.4.4. Such use does not overburden any CMS information system resources;
4.12.4.5. Such use is not otherwise prohibited under this policy; and
4.12.4.6. Any use of organizational Internet and email resources shall be made with the understanding that such use is not secure, private or anonymous.

The following uses of organization-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited:
4.12.4.7. Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace;
4.12.4.8. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords;
4.12.4.9. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity;
4.12.4.10. All email communications to groups of employees that are subject to approval prior to distribution and have not been approved by the organization (e.g., retirement announcements, union notices or announcements, charitable solicitations); and
4.12.4.11. Employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees.

All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of organization-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that employees desire to protect their privacy, employees shall not use organization-owned or leased equipment and resources.

Guidance

Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST SP 800-18 provides guidance on preparing rules of behavior.

Applicability: All	**References:** ARS: PL-4; FISCAM: TSP-3.3.2; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.5; NIST 800-53/53A: PL-4; PISP: 4.12.4	**Related Controls:**

ASSESSMENT PROCEDURE: PL-4.1

Assessment Objective

Determine if:
(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;

(ii) the organization makes the rules available to all information system users;
(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and
(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records.
Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior.

PL-4(CMS-1) – Enhancement (High)

Control

Define user roles and expectations for system and network use.

Applicability: All	**References:** ARS: PL-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-4(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;
(ii) the organization makes the rules available to all information system users;
(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and
(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records to determine user roles and expectations for system and network use are defined.
Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior to determine user roles and expectations for system and network use are defined.

PL-4(CMS-2) – Enhancement (High)

Control

Electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

Applicability: All	**References:** ARS: PL-4(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-4(CMS-2).1

Assessment Objective

Determine if:
(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;
(ii) the organization makes the rules available to all information system users;
(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and
(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records to determine electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).
Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior to determine electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

PL-5 – Privacy Impact Assessment (PIA) (High)

Control

PIAs shall be conducted for CMS information systems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandum M-03-22, and the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations.

Guidance

OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

Applicability: All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC	**References:** ARS: PL-5; HSPD 7: J(35); NIST 800-53/53A: PL-5; PISP: 4.12.5	**Related Controls:**

ASSESSMENT PROCEDURE: PL-5.1

Assessment Objective

Determine if:
(i) the organization conducts a privacy impact assessment on the information system in accordance with OMB policy; and
(ii) the privacy impact assessment is consistent with federal legislation and OMB policy.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing privacy impact assessments on the information system; appropriate federal legislation and OMB policy; privacy impact assessment; other relevant documents or records.

PL-6 – Security-Related Activity Planning (High)

Control

Security-related activities affecting the information system shall be planned and coordinated before being performed in order to reduce the impact on CMS operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing / exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Guidance

Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Applicability: All	**References:** ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6	**Related Controls:**

ASSESSMENT PROCEDURE: PL-6.1

Assessment Objective

Determine if:
(i) the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations, organizational assets, and individuals; and
(ii) the organization's advance planning and coordination of security-related activities includes both emergency and non-emergency situations.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.

Personnel Security (PS) – *Operational*

PS-1 – Personnel Security Policy and Procedures (High)		
Control CMS information systems shall employ personnel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines. Procedures shall be developed to guide the implementation of personnel security controls.		
Guidance The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.		
Applicability: All	**References:** ARS: PS-1; FISCAM: TSD-1.3.3; IRS-1075: 5.6.2.1#1.1-2; NIST 800-53/53A: PS-1; PISP: 4.13.1	**Related Controls:**
ASSESSMENT PROCEDURE: PS-1.1		
Assessment Objective Determine if: (i) the organization develops and documents personnel security policy and procedures; (ii) the organization disseminates personnel security policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review personnel security policy and procedures; and (iv) the organization updates personnel security policy and procedures when organizational review indicates updates are required. **Assessment Methods And Objects** **Examine:** Personnel security policy and procedures, other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.		
ASSESSMENT PROCEDURE: PS-1.2		
Assessment Objective Determine if: (i) the personnel security policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the personnel security policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the personnel security procedures address all areas identified in the personnel security policy and address achieving policy-compliant implementations of all associated security controls. **Assessment Methods And Objects** **Examine:** Personnel security policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.		
PS-1(FIS-1) – Enhancement (High)		
Control Staff's performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.		
Applicability: All	**References:** FISCAM: TSD-2.2.1	**Related Controls:**
ASSESSMENT PROCEDURE: PS-1(FIS-1).1		
Assessment Objective Determine if the organization monitors staff performance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are carried out. **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes). **Interview:** Management and subordinate personnel.		
PS-1(FIS-2) – Enhancement (High)		
Control Regularly scheduled vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.		
Applicability: All	**References:** FISCAM: TSD-1.1.7, TSP-4.1.4, TSP-4.1.5	**Related Controls:**

ASSESSMENT PROCEDURE: PS-1(FIS-2).1

Assessment Objective

Determine if the organization regularly schedules vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.

Assessment Methods And Objects

Examine: Personnel records to identify individuals who have not taken vacation or sick leave in the past year.
Examine: Staff assignment records and determine whether job and shift rotations occur.
Examine: Vacation and job rotation policies and procedures.
Interview: Information system management and users.

PS-1(FIS-3) – Enhancement (High)

Control

Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes. Employees are made aware of their job descriptions.

Applicability: All	**References:** FISCAM: TSD-1.2.2, TSD-1.3.1, TSP-4.2.1, TSS-2.1.2, TSS-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: PS-1(FIS-3).1

Assessment Objective

Determine if:
(i) the organizational documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes.
(ii) the organization makes the employees aware of their job descriptions.

Assessment Methods And Objects

Examine: Effective dates of the position descriptions and determine whether they are current.
Examine: Job descriptions for several positions in organizational units and for user security administrators.
Examine: Job descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
Interview: Management personnel.

PS-2 – Position Categorization (High)

Control

A criticality / sensitivity rating (e.g., non-sensitive, national security, public trust) shall be assigned to all positions within the organization. The criticality / sensitivity rating shall be in compliance with 5 CFR 731.106(a), Executive Orders 10450 and 12968, NSPD-1, HSPD-7, and HSPD-12 and consistent with OPM policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating. All criticality / sensitivity ratings must be submitted to the DHHS HR department and CMS' personnel security department.

Guidance

Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Applicability: All	**References:** ARS: PS-2; IRS-1075: 5.6.2.1#1.3; NIST 800-53/53A: PS-2; PISP: 4.13.2	**Related Controls:**

ASSESSMENT PROCEDURE: PS-2.1

Assessment Objective

Determine if:
(i) the organization assigns a risk designations to all positions within the organization;
(ii) the organization establishes a screening criteria for individuals filling organizational positions;
(iii) the risk designations for the organizational positions are consistent with applicable federal regulations and OPM policy and guidance;
(iv) the organization defines the frequency of risk designation reviews and updates for organizational positions; and
(v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan; records of risk designation reviews and updates; other relevant documents or records.

PS-2(0) – Enhancement (High)

Control

Review and revise position risk designations every 365 days.

Applicability: All	References: ARS: PS-2(0); NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:

ASSESSMENT PROCEDURE: PS-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan (for organization-defined frequency for review of position categorizations); records of risk designation reviews and updates; other relevant documents or records.

PS-3 – Personnel Screening (High)

Control

Prior to being granted access, all employees and contractors who require access to CMS information or information systems shall be screened and reinvestigated periodically, consistent with the criticality / sensitivity rating of the position. For prospective employees, references background checks shall be performed before issuance of a User ID. Security agreements shall be required for employees and contractors assigned to work with mission critical information.

Guidance

Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and SP 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.

Applicability: All	References: ARS: PS-3; FISCAM: TSP-4.1.1, TSP-4.1.2; IRS-1075: 5.6.2.1#1.4; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:

ASSESSMENT PROCEDURE: PS-3.1

Assessment Objective

Determine if:

(i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and

(ii) the personnel screening is consistent with appropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 800-78; other relevant documents or records.

PS-3(0) – Enhancement (High)

Control

Perform criminal history check for all persons prior to employment.

Applicability: All	References: ARS: PS-3(0); FISCAM: TSP-4.1.2; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:

ASSESSMENT PROCEDURE: PS-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 800-78; other relevant documents or records.

PS-3(CMS-1) – Enhancement (High)

Control

Require personnel to obtain and hold a high-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook.

Applicability: All	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:

ASSESSMENT PROCEDURE: PS-3(CMS-1).1

Assessment Objective

Determine if:

(i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and

(ii) the personnel screening is consistent with appropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; and other relevant documents or records to determine that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.
Interview: Personnel with personnel screening responsibilities to confirm that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

PS-4 – Personnel Termination (High)

Control

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information and information systems is removed upon personnel termination. Termination procedures shall address:
4.13.4.1. Exit interviews;
4.13.4.2. Retrieval of all organizational information system-related property;
4.13.4.3. Notification to security management;
4.13.4.4. Revocation of all system access privileges;
4.13.4.5. Immediately escorting employees terminated for cause out of organization facilities; and
4.13.4.6. Hard disk back up and sanitization before re-issuance.

Appropriate personnel shall have access to official records created by the terminated employee that are stored on organizational information systems.

Guidance

Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Applicability: All	**References:** ARS: PS-4; FISCAM: TAC-2.1.6, TSP-4.1.6; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: 5.6.2.1#1.5; NIST 800-53/53A: PS-4; PISP: 4.13.4	**Related Controls:**

ASSESSMENT PROCEDURE: PS-4.1

Assessment Objective

Determine if:
(i) the organization terminates information system access upon termination of individual employment;
(ii) the organization conducts exit interviews of terminated personnel;
(iii) the organization retrieves all organizational information system-related property from terminated personnel; and
(iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities.

PS-4(CMS-1) – Enhancement (High)

Control

Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

Applicability: All	**References:** ARS: PS-4(CMS-1); FISCAM: TAC-3.2.C.4	**Related Controls:**

ASSESSMENT PROCEDURE: PS-4(CMS-1).1

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.
Interview: Personnel with termination responsibilities to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

PS-5 – Personnel Transfer (High)

Control

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information or information systems no longer required in the new assignment is

terminated upon personnel transfer. Transfer procedures shall address:

4.13.5.1. Re-issuing appropriate organizational information system-related property (e.g., keys, identification cards, building passes);
4.13.5.2. Notification to security management;
4.13.5.3. Closing obsolete accounts and establishing new accounts; and
4.13.5.4. Revocation of all system access privileges (if applicable).

Guidance

Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts.

Applicability: All	**References:** ARS: PS-5; FISCAM: TAC-2.1.6, TSP-4.1.6; IRS-1075: 5.6.2.1#1.6; NIST 800-53/53A: PS-5; PISP: 4.13.5	**Related Controls:**

ASSESSMENT PROCEDURE: PS-5.1

Assessment Objective

Determine if:
(i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and
(ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

PS-6 – Access Agreements (High)

Control

Individuals who require access to CMS information or information systems shall be required to complete and sign appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements.

Guidance

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Applicability: All	**References:** ARS: PS-6; FISCAM: TSP-4.1.3; IRS-1075: 5.6.2.1#1.7; NIST 800-53/53A: PS-6; PISP: 4.13.6	**Related Controls:**

ASSESSMENT PROCEDURE: PS-6.1

Assessment Objective

Determine if:
(i) the organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access;
(ii) organizational personnel sign access agreements;
(iii) the organization defines the frequency of reviews and updates for access agreements; and
(iv) the organization reviews and updates the access agreements in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records.

PS-6(0) – Enhancement (High)

Control

Access agreements are reviewed and updated as part of the system accreditation or when a contract is renewed or extended.

Applicability: All	**References:** ARS: PS-6(0); NIST 800-53/53A: PS-6; PISP: 4.13.6	**Related Controls:**

ASSESSMENT PROCEDURE: PS-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan (for organization-defined

frequency for access agreement reviews); access agreements; records of access agreement reviews and updates; other relevant documents or records.

PS-7 – Third-Party Personnel Security (High)

Control

Personnel security controls employed by external service providers and third parties shall be documented, agreed to, implemented effectively, and monitored for compliance and shall include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements. Personnel security controls employed by service providers and third parties shall be compliant with CMS IS policies and procedures, and consistent with NIST SP 800-35.

Guidance

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST SP 800-35 provides guidance on information technology security services.

Applicability: All	**References:** ARS: PS-7; IRS-1075: 5.6.2.1#1.8; NIST 800-53/53A: PS-7; PISP: 4.13.7	**Related Controls:**

ASSESSMENT PROCEDURE: PS-7.1

Assessment Objective

Determine if:
(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management);
(ii) the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST SP 800-35; and
(iii) the organization monitors third-party provider compliance with personnel security requirements.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities; third-party providers.

PS-7(CMS-1) – Enhancement (High)

Control

Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.

Applicability: All	**References:** ARS: PS-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PS-7(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management); and
(ii) the organization monitors third-party provider compliance with personnel security requirements.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records to determine the access provided to contractors and defining security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.
Interview: Personnel with third party security responsibilities to determine that the access provided to contractors are defined within the security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.

PS-8 – Personnel Sanctions (High)

Control

The organization shall enforce formal personnel sanctions process for personnel who fail to comply with established CMS IS policies and procedures. The employee sanction process shall be consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines.

Guidance

The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Applicability: All	References: ARS: PS-8; HIPAA: 164.308(a)(1)(ii)(C); NIST 800-53/53A: PS-8; PISP: 4.13.8	Related Controls:

ASSESSMENT PROCEDURE: PS-8.1

Assessment Objective

Determine if:
(i) the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
(ii) the personnel sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records.

PS-CMS-1 – Review System Access during Extraordinary Personnel Circumstances (High)

Control

Access to CMS information and information systems shall be reviewed during extraordinary personnel circumstances and limited as deemed necessary.

Guidance

A death in the family or other personal problems could be considered extraordinary personal circumstances. For some personnel, recovery from a difficult time may take longer than usual and management must consider the circumstances on a case by case basis.

Applicability: All	References: ARS: PS-9; PISP: 4.13.9	Related Controls:

ASSESSMENT PROCEDURE: PS-CMS-1.1

Assessment Objective

Determine if the organization manages personnel with extraordinary personal circumstances.

Assessment Methods And Objects

Examine: Personnel security policy and procedures; other relevant documents or records determine system access during extraordinary personnel circumstances is reviewed and access is limited as deemed necessary.

Interview: Organizational personnel with personnel security responsibilities to determine system access during extraordinary personnel circumstances is reviewed and access is limited as deemed necessary.

PS-CMS-2 – Designate an Information System Security Officer (ISSO) / System Security Officer (SSO) (High)

Control

An Information System Security Officer (ISSO) / System Security Officer (SSO) shall be designated for each business component with roles and responsibilities of the position clearly defined.

Guidance

A good reference set for defining the Information System Security Officer (ISSO) / System Security Officer (SSO) responsibilities are the NIST SPs. Specific responsibilities should be developed to protect CMS information systems and data.

Applicability: All	References: ARS: PS-10; FISCAM: TSP-3.1.1, TSP-3.1.2; HIPAA: 164.308(a)(2); PISP: 4.13.10	Related Controls:

ASSESSMENT PROCEDURE: PS-CMS-2.1

Assessment Objective

Determine if the organization has documented the roles and responsibilities of appointed ISSO / SSO.

Assessment Methods And Objects

Examine: Personnel security policy and procedures; other relevant documents or records to determine an ISSO / SSO is designated for each component with roles and responsibilities of the position clearly defined.

Interview: Organizational personnel with personnel security responsibilities to determine an ISSO / SSO is designated for each component with roles and responsibilities of the position clearly defined.

Risk Assessment (RA) – *Management*

RA-1 – Risk Assessment Policy and Procedures (High)

Control

All CMS applications and systems shall be covered by an IS RA. The RA shall be consistent with NIST SP 800-30. Formal documented procedures shall be developed, disseminated, and reviewed / updated periodically to facilitate the implementation of the RA policy and associated RA controls. The procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-30 provides guidance on the assessment of risk. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: RA-1; FISCAM: TAC-3.1.A.2; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075: 5.6.1.1#1.1-2; NIST 800-53/53A: RA-1; PISP: 4.14.1	**Related Controls:**

ASSESSMENT PROCEDURE: RA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents risk assessment policy and procedures;
(ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review risk assessment policy and procedures; and
(iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.

ASSESSMENT PROCEDURE: RA-1.2

Assessment Objective

Determine if:
(i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.

RA-2 – Security Categorization (High)

Control

CMS information systems and the information processed, stored, or transmitted by the systems shall be categorized in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to the, CMS System Security Level by Information Type. The security categorization (including supporting rationale) shall be explicitly documented. Designated senior-level officials within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the CMS CIO, CISO, and Business Owners.

All CMS information systems categorized as high or moderate shall be considered sensitive or to contain sensitive information. All CMS information systems categorized as low shall be considered non-sensitive or to contain non-sensitive information. All CMS information systems shall implement minimum security requirements and controls as established in the current CMS IS Standards, based on security categorization of the system.

Guidance

The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST SP 800-60 provides guidance on determining the security categories of the

information types resident on the information system.

Applicability: All	**References:** ARS: RA-2; FISCAM: TAC-1.1; HSPD 7: D(8); IRS-1075: 4.1#2; NIST 800-53/53A: RA-2; PISP: 4.14.2	**Related Controls:** MP-4, SC-7

ASSESSMENT PROCEDURE: RA-2.1

Assessment Objective

Determine if:
(i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners;
(ii) the security categorization is consistent with FIPS 199 and NIST SP 800-60;
(iii) the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts;
(iv) the organization includes supporting rationale for impact-level decisions as part of the security categorization; and
(v) designated, senior-level organizational officials review and approve the security categorization of the information system.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST SP 800-60; information system security plan; other relevant documents or records.
Interview: Organizational personnel with security categorization and risk assessment responsibilities.

RA-3 – Risk Assessment (RA) (High)

Control

An assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that support the operations and assets of CMS shall be performed, both within CMS and by external parties that manage / operate information or information systems for CMS. The RA shall be in accordance with current CMS Procedures. Based on the operation of the information system, the RA shall take into account vulnerabilities, threat sources, and security controls in place to determine the resulting level of residual risk posed to CMS operations, CMS assets, CMS information, or individuals.

Any findings from reviews of CMS systems shall be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses shall be documented by the Business Owner or external party and addressed by mitigating the risk, accepting the risk with explanation or submitting Corrective Action Plan (CAP). These findings shall be subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST SP 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Applicability: All	**References:** ARS: RA-3; FISCAM: TAC-3.1.A.2, TSP-1.1.2, TSP-1.1.3, TSP-5.1.4; HIPAA: 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3, 6.3.3#2; NIST 800-53/53A: RA-3; PISP: 4.14.3	**Related Controls:**

ASSESSMENT PROCEDURE: RA-3.1

Assessment Objective

Determine if:
(i) the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and
(ii) the risk assessment is consistent with the NIST SP 800-30.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST SP 800-30; other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.

RA-3(CMS-1) – Enhancement (High)

Control

Perform an IS RA for the system, and document the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

Applicability: All	References: ARS: RA-3(CMS-1); FISCAM: TAC-1.1, TAC-1.2, TSS-2.2.4; HIPAA: 164.306(a)(2); HSPD 7: D(8), F(19)	Related Controls:

ASSESSMENT PROCEDURE: RA-3(CMS-1).1

Assessment Objective

Determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties).

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; information system security plan (for organization-defined frequency for risk assessment updates); records of risk assessment updates; NIST SP 800-30; other relevant documents or records to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

Interview: Organizational personnel with risk assessment responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

RA-4 – Risk Assessment Update (High)

Control

The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation.

Guidance

The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates.

Applicability: All	References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4	Related Controls:

ASSESSMENT PROCEDURE: RA-4.1

Assessment Objective

Determine if:

(i) the organization defines the frequency of risk assessment updates;

(ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system;

(iii) the risk assessment update is consistent with the NIST SP 800-30; and

(iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing risk assessment updates; risk assessment; information system security plan; records of risk assessment updates; NIST SP 800-30; other relevant documents or records.

RA-5 – Vulnerability Scanning (High)

Control

Appropriate vulnerability assessment tools and techniques shall be implemented by the organization. Selected personnel shall be trained in their use and maintenance. The organization shall conduct periodic testing of its security posture by scanning its information systems with vulnerability tools. The information obtained from the vulnerability scanning process shall be shared with appropriate personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems. The activities of employees using organization Internet and email resources shall be subject to monitoring by system or security personnel without notice.

Guidance

Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST SP 800-42 provides guidance on

network security testing. NIST SP 800-40 (Version 2) provides guidance on patch and vulnerability management.

Applicability: All	References: ARS: RA-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5; PISP: 4.14.5	Related Controls:

ASSESSMENT PROCEDURE: RA-5.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of vulnerability scans within the information system;
(ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported;
(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact;
(iv) the organization performs network vulnerability scanning in accordance with NIST SP 800-42; and
(v) the organization handles patch and vulnerability management in accordance with NIST SP 800-40.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.

RA-5(0) – Enhancement (High)

Control

Utilize appropriate vulnerability scanning tools and techniques to scan for vulnerabilities in the information system every 90 days or when significant new vulnerabilities are identified and reported.

Applicability: All	References: ARS: RA-5(0); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5; PISP: 4.14.5	Related Controls:

ASSESSMENT PROCEDURE: RA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for vulnerability scanning); vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.

RA-5(1) – Enhancement (High)

Control

Vulnerability scanning tools must include the capability to readily update the list of vulnerabilities scanned.

Applicability: All	References: ARS: RA-5(1); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5(1)	Related Controls:

ASSESSMENT PROCEDURE: RA-5(1).1

Assessment Objective

Determine if:
(i) the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned; and
(ii) the vulnerability scanning tools retrieve updated lists of information system vulnerabilities from the National Vulnerability Database (NVD).

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning tools and techniques documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.
Test: Vulnerability scanning capability and associated scanning tools.

RA-5(2) – Enhancement (High)

Control

Update the list of system vulnerabilities scanned every 365 days or when significant new vulnerabilities are identified and reported.

Applicability: All	References: ARS: RA-5(2); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5(2)	Related Controls:

ASSESSMENT PROCEDURE: RA-5(2).1

Assessment Objective

Determine if:
(i) the organization defines the frequency of updates for information system vulnerabilities scanned; and
(ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when significant new vulnerabilities are identified and reported.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records.

RA-5(3) – Enhancement (High)

Control

Perform internal network penetration testing as needed but no less than once a year, in accordance with the CMS IS procedures. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.

Applicability: All	**References:** ARS: RA-5(3); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5(3)	**Related Controls:**

ASSESSMENT PROCEDURE: RA-5(3).1

Assessment Objective

Determine if:
(i) the organization implements procedures that can demonstrate the breadth of scan coverage (including information system components scanned); and
(ii) the organization implements procedures that can demonstrate the depth of scan coverage (including vulnerabilities checked).

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and information system components checked; other relevant documents or records.(Optional)

RA-5(CMS-1) – Enhancement (High)

Control

Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once a year, in accordance with CMS IS procedures. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.

Applicability: All	**References:** ARS: RA-5(CMS-1); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24)	**Related Controls:**

ASSESSMENT PROCEDURE: RA-5(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines the frequency of vulnerability scans within the information system;
(ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported; and
(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for vulnerability scanning); vulnerability scanning results; patch and vulnerability management records; other relevant documents or records to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE) naming convention.

Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE) naming convention.

System and Services Acquisition (SA) – *Management*

SA-1 – System and Services Acquisition Policy and Procedures (High)

Control

Documented procedures shall be developed and implemented effectively to facilitate the implementation of the system and services acquisition security controls in all system and services acquisitions. Procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and services acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: SA-1; IRS-1075: 5.6.1.3#1.1-2; NIST 800-53/53A: SA-1; PISP: 4.15.1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and services acquisition policy and procedures;
(ii) the organization disseminates system and services acquisition policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and services acquisition policy and procedures; and
(iv) the organization updates system and services acquisition policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.

ASSESSMENT PROCEDURE: SA-1.2

Assessment Objective

Determine if:
(i) the system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and services acquisition policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and services acquisition procedures address all areas identified in the system and services acquisition policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.

SA-1(IRS-1) – Enhancement (High)

Control

For FTI, develop, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes IRS documents received and identified by:
(a) taxpayer name
(b) tax year(s)
(c) type of information (e.g., revenue agent reports, Form 1040, work papers)
(d) the reason for the request
(e) date requested
(f) date received
(g) exact location of the FTI
(h) who has had access to the data and
(i) if disposed of, the date and method of disposition.

Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	**References:** IRS-1075: 3.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-1(IRS-1).1

Assessment Objective

Determine if the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes IRS documents received and

identified by:
(a) taxpayer name
(b) tax year(s)
(c) type of information (e.g., revenue agent reports, Form 1040, work papers)
(d) the reason for the request
(e) date requested
(f) date received
(g) exact location of the FTI
(h) who has had access to the data and
(i) if disposed of, the date and method of disposition.

Assessment Methods And Objects

Examine: Organizational documentation that contains the development, dissemination and review/updates to FTI IRS documents received that show:
(a) taxpayer name
(b) tax year(s)
(c) type of information (e.g., revenue agent reports, Form 1040, work papers)
(d) the reason for the request
(e) date requested
(f) date received
(g) exact location of the FTI
(h) who has had access to the data and
(i) if disposed of, the date and method of disposition.

SA-2 – Allocation of Resources (High)

Control

As part of the capital planning and investment control processes, CMS or the external organization shall determine, document, and allocate the resources required to protect CMS information systems adequately. IS requirements shall be included in mission / business case planning, and a separate line item shall be established in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Guidance

The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST SP 800-65 provides guidance on integrating security into the capital planning and investment control process.

Applicability: All	**References:** ARS: SA-2; NIST 800-53/53A: SA-2; PISP: 4.15.2	**Related Controls:**

ASSESSMENT PROCEDURE: SA-2.1

Assessment Objective

Determine if:
(i) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system;
(ii) the organization determines security requirements for the information system in mission/business case planning;
(iii) the organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation; and
(iv) the organization's programming and budgeting process is consistent with NIST SP 800-65.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST SP 800-65; other relevant documents or records.
Interview: Organizational personnel with capital planning and investment responsibilities.

SA-3 – Life Cycle Support (High)

Control

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

Guidance

NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Applicability: All	**References:** ARS: SA-3; FISCAM: TAY-1.2.1, TCC-1.1.2; NIST 800-53/53A: SA-3; PISP: 4.15.3	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3.1

Assessment Objective

Determine if:

(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and
(ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation; other relevant documents or records.
Interview: Organizational personnel with information security and system life cycle development responsibilities.

SA-3(CMS-1) – Enhancement (High)

Control

Must comply with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

Applicability: All	**References:** ARS: SA-3(CMS-1); FISCAM: TCC-1.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3(CMS-1).1

Assessment Objective

Determine if:
(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and
(ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation; other relevant documents or records to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.
Interview: Organizational personnel with information security and system life cycle development responsibilities to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

SA-3(FIS-1) – Enhancement (High)

Control

Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.

Applicability: All	**References:** FISCAM: TCC-2.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3(FIS-1).1

Assessment Objective

Determine if the organizational detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.

Assessment Methods And Objects

Examine: Design system specifications.
Examine: Pertinent policies and procedures.
Interview: Programmer and programming supervisor.

SA-4 – Acquisitions (High)

Control

Security requirements and/or security specifications shall be included, either explicitly or by reference, in all information system acquisition contracts based on an assessment of risk in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

Solicitation Documents
Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required:
4.15.4.1. Security capabilities;
4.15.4.2. Design and development processes;
4.15.4.3. Test and evaluation procedures; and
4.15.4.4. Documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats / vulnerabilities are identified and as new technologies are implemented

Use of Evaluated and Validated Products
For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to

products that have been evaluated and validated through one or more of the following sources:

1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

Configuration Settings and Implementation Guidance
The information system required documentation shall include security configuration settings, including documentation explaining exceptions to the standard, and security implementation guidance.

Guidance

Solicitation Documents
The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST SP 800-36 provides guidance on the selection of information security products. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Information System Documentation
The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

Use of Tested, Evaluated, and Validated Products
NIST SP 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.

Configuration Settings and Implementation Guidance
The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on configuration settings for information technology products.

Applicability: All	**References:** ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4	**Related Controls:**

ASSESSMENT PROCEDURE: SA-4.1

Assessment Objective

Determine if:
(i) the organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards;
(ii) the organization's acquisition of commercial information technology products is consistent with NIST SP 800-23;
(iii) references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST SP 800-70; and
(iv) acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe:
- required security capabilities;
- required design and development processes;
- required test and evaluation procedures; and
- required documentation.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.
Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.

SA-4(1) – Enhancement (High)

Control

Ensure solicitation documents require that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Applicability: All	**References:** ARS: SA-4(1); NIST 800-53/53A: SA-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-4(1).1

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.

SA-4(CMS-1) – Enhancement (High)

Control

Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

Applicability: All	**References:** ARS: SA-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-4(CMS-1).1

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records to determine that all contracts and Statements of Work (SOW) that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities to determine that all contracts and SOW that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

SA-5 – Information System Documentation (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

Guidance

Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Applicability: All	**References:** ARS: SA-5; FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1, TSD-3.1.2, TSD-3.1.3, TSP-3.3.2; IRS-1075: 5.6.1.3#1.3; NIST 800-53/53A: SA-5; PISP: 4.15.5	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5.1

Assessment Objective

Determine if:

(i) the organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system;

(ii) the organization makes available information on configuring, installing, and operating the information system; and

(iii) the organization makes available information on effectively using the security features in the information system.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; other relevant documents or records.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.

SA-5(1) – Enhancement (High)		
Control Ensure that system documentation describes the functional properties of the security controls implemented within the information system with sufficient detail to facilitate analysis and testing of the controls.		
Applicability: All	**References:** ARS: SA-5(1); NIST 800-53/53A: SA-5(1)	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(1).1		
Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records. **Interview:** Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system.		
SA-5(2) – Enhancement (High)		
Control Ensure that system documentation describes the design and implementation details of the security controls implemented within the information system with sufficient detail to permit analysis and testing of the controls.		
Applicability: All	**References:** ARS: SA-5(2); NIST 800-53/53A: SA-5(2)	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(2).1		
Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records. **Interview:** Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.		
SA-5(CMS-1) – Enhancement (High)		
Control Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.		
Applicability: All	**References:** ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(CMS-1).1		
Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance; and required personnel training to include administrators and users. **Interview:** Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance; and required personnel training to include administrators and users.		
SA-5(CMS-2) – Enhancement (High)		
Control Maintain an updated list of related system operations and security documentation.		
Applicability: All	**References:** ARS: SA-5(CMS-2); FISCAM: TSD-1.1.6	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(CMS-2).1

Assessment Objective

Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization maintains an updated list of related system's operations and security documentation.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization maintains an updated list of related system's operations and security documentation.

SA-5(CMS-3) – Enhancement (High)

Control

Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.

Applicability: All	**References:** ARS: SA-5(CMS-3); FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(CMS-3).1

Assessment Objective

Determine if responsible parties within the organization periodically review system and services acquisition policy and procedures.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization updates documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine if the organization updates documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.

SA-5(CMS-4) – Enhancement (High)

Control

Document the system's configuration, and procedures in support of system access administration and operations.

Applicability: All	**References:** ARS: SA-5(CMS-4); FISCAM: TSD-1.1.6	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(CMS-4).1

Assessment Objective

Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization documents the system's configuration and procedures in support of system access administration and operations.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization documents the system's configuration and procedures in support of system access administration and operations.

SA-5(FIS-1) – Enhancement (High)

Control

Goals are established by senior management on the availability of data processing and on-line services. Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.

Applicability: All	**References:** FISCAM: TSC-2.4.6, TSC-2.4.9	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(FIS-1).1

Assessment Objective

Determine if the organizational goals are established by senior management on the availability of data processing and on-line services. Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation.

Interview: Senior management, data processing management, and user management.

SA-5(FIS-2) – Enhancement (High)

Control

Records are maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.

Applicability: All	**References:** FISCAM: TSC-2.4.7, TSC-2.4.8	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(FIS-2).1

Assessment Objective

Determine if the organizational records are maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation.

Interview: Senior management, data processing management, and user management.

SA-6 – Software Usage Restrictions (High)

Control

All software or shareware and associated documentation used on CMS information systems shall be deployed and maintained in accordance with appropriate license agreements and copyright laws. Software associated documentation protected by quantity licenses shall be managed through a tracking system to control copying and distribution. All other uses not specifically authorized by the license agreement shall be prohibited. The use of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Guidance

Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Applicability: All	**References:** ARS: SA-6; FISCAM: TCC-2.3.1; IRS-1075: 4.7.3#1.2; NIST 800-53/53A: SA-6; PISP: 4.15.6	**Related Controls:**

ASSESSMENT PROCEDURE: SA-6.1

Assessment Objective

Determine if:

(i) the organization complies with software usage restrictions; and

(ii) the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records.

Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.

SA-6(FIS-1) – Enhancement (High)

Control

Implementation orders, including effective date, are provided to all locations where they are maintained on file.

Applicability: All	**References:** FISCAM: TCC-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: SA-6(FIS-1).1

Assessment Objective

Determine if the organization provides to all locations software implementation orders, including effective date, where the orders are maintained on file.

Assessment Methods And Objects

Examine: Implementation orders.
Examine: Pertinent policies and procedures.
Interview: Information system and security administrators.

SA-7 – User Installed Software (High)

Control

All users shall be restricted from downloading or installing software, unless explicitly authorized in writing by the CIO or his/her designated representative. Users that have been granted such authorization may download and install only organization-approved software. The use of install-on-demand software shall be restricted.

Guidance

If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Applicability: All	**References:** ARS: SA-7; FISCAM: TCC-1.3.1; NIST 800-53/53A: SA-7; PISP: 4.15.7	**Related Controls:**

ASSESSMENT PROCEDURE: SA-7.1

Assessment Objective

Determine if:
(i) the organization enforces explicit rules governing the installation of software by users;
(ii) unauthorized software is present on the system; and
(iii) the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary action.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records.
Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.
Test: Enforcement of rules for user installed software on the information system; information system for prohibited software.

SA-7(CMS-1) – Enhancement (High)

Control

If user installed software is authorized in writing by the CIO or his/her designated representative, ensure that business rules and technical controls enforce the documented authorizations and prohibitions.

Applicability: All	**References:** ARS: SA-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-7(CMS-1).1

Assessment Objective

Determine if:
(i) the organization enforces explicit rules governing the installation of software by users; and
(ii) unauthorized software is present on the system.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records to determine that policies exist that ensure business rules and technical controls enforce the documented authorizations and prohibitions.
Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine that policies exist that ensure business rules and technical controls enforce the documented authorizations and prohibitions.
Test: Enforcement of rules for user installed software on the information system; information system for prohibited software to determine authorizations and prohibitions.

SA-8 – Security Engineering Principles (High)

Control

CMS information systems shall be designed and implemented using accepted security engineering principles.

Guidance

NIST SP 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to

system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

Applicability: All	**References:** ARS: SA-8; FISCAM: TAY-2.1.1, TAY-2.2.1, TCC-2.1.3; NIST 800-53/53A: SA-8; PISP: 4.15.8	**Related Controls:**

ASSESSMENT PROCEDURE: SA-8.1

Assessment Objective

Determine if:
(i) the organization designs and implements the information system using security engineering principles; and
(ii) the organization considers security design principles in the development and implementation of the information system consistent with NIST SP 800-27.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST SP 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.

SA-8(0) – Enhancement (High)

Control

Design and implement the information system using the security engineering principles detailed in NIST SP 800-27 Rev. A, Engineering Principles for IT Security (A Baseline for Achieving Security).

Applicability: All	**References:** ARS: SA-8(0); FISCAM: TCC-2.1.3; NIST 800-53/53A: SA-8; PISP: 4.15.8	**Related Controls:**

ASSESSMENT PROCEDURE: SA-8(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST SP 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.

SA-9 – External Information System Services (High)

Control

All external information system services shall include specific provisions requiring the service provider to comply with CMS IS policies, standards, and guidelines; and shall be monitored for compliance. CMS shall define the remedies for any loss, disruption, or damage caused by the service provider's failure to comply. Service providers shall be prohibited from outsourcing any system function overseas, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representatives with concurrence from CMS' personnel security department.

Guidance

An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on the security considerations in the system development life cycle.

Applicability: All	**References:** ARS: SA-9; FISCAM: TAY-1.3.1; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4; NIST 800-53/53A: SA-9; PISP: 4.15.9	**Related Controls:** CA-3

ASSESSMENT PROCEDURE: SA-9.1

Assessment Objective

Determine if:
(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;
(ii) the organization monitors security control compliance;

(iii) the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions; and

(iv) the security controls employed by providers of external information system services are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

SA-9(CMS-1) – Enhancement (High)

Control

If service providers are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas, ensure that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Applicability: All	**References:** ARS: SA-9(CMS-1); HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-9(CMS-1).1

Assessment Objective

Determine if the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

SA-9(HIP-1) – Enhancement (High)

Control

A covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a).)

Applicability: All	**References:** HIPAA: 164.308(b)(1), 164.308(b)(4), 164.314(a)(1)(i), 164.314(a)(2)(i), 164.314(a)(2)(i)(A), 164.314(a)(2)(i)(B), 164.314(a)(2)(i)(C), 164.314(a)(2)(i)(D), 164.314(a)(2)(ii)(A)(1), 164.314(a)(2)(ii)(A)(2), 164.314(a)(2)(ii)(B)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-9(HIP-1).1

Assessment Objective

Determine if the organizational covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a))

Assessment Methods And Objects

Examine: Organizational documentation meets the requirements set forth in HIPAA regulations (See HIPAA 164.308(b) and 164.314(a)) for a covered entity.

Interview: Organizational personnel maintaining covered entity documentation follow requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a).)

SA-10 – Developer Configuration Management (High)

Control

Information system developers shall develop, document, and implement a configuration management plan for each information system under development. The configuration management plan shall address change control mechanisms during development, change authorization requirements, and security flaw identification, tracking, and remediation processes.

Guidance

This control also applies to the development actions associated with information system changes.

Applicability: All	**References:** ARS: SA-10; NIST 800-53/53A: SA-10; PISP: 4.15.10	**Related Controls:**

ASSESSMENT PROCEDURE: SA-10.1

Assessment Objective

Determine if the organization requires that information system developers (and systems integrators) create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records.

SA-11 – Developer Security Testing (High)

Control

Information system developers shall develop, document, and implement a security test and evaluation (ST&E) plan for each information system under development in accordance with, but not limited to the, current CMS Procedures. The developer security test results shall be documented.

Guidance

Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system.

Applicability: All	**References:** FISCAM: TCC-2.1.5; NIST 800-53/53A: SA-11	**Related Controls:** CA-2, CA-4

ASSESSMENT PROCEDURE: SA-11.1

Assessment Objective

Determine if the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; other relevant documents or records.

SA-11(CMS-1) – Enhancement (High)

Control

If the Security Test and Evaluation (ST&E) results are used in support of the security C&A process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the security testing and after selective verification of the results.

Applicability: All	**References:** ARS: SA-11(CMS-1); FISCAM: TCC-2.1.8	**Related Controls:**

ASSESSMENT PROCEDURE: SA-11(CMS-1).1

Assessment Objective

Determine if the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; other relevant documents or records to determine that no security relevant modifications of the information system has been made subsequent to the security testing and after selective verification of the results if the security test and evaluation results are used in support of the security C&A process for the information system.

Interview: Organizational personnel with developer security testing responsibilities to determine that no security relevant modifications of the information system has been made subsequent to the security testing and after selective verification of the results if the security test and evaluation results are used in support of the security C&A process for the information system.

SA-11(CMS-2) – Enhancement (High)

Control

Use hypothetical data when executing test scripts.

Applicability: All	**References:**	**Related Controls:**

ASSESSMENT PROCEDURE: SA-11(CMS-2).1

Assessment Objective

Determine if the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records to determine hypothetical data is used when executing test scripts.

Interview: Personnel with system and information integrity responsibilities to determine hypothetical data is used when executing test scripts.
Test: Information systems to determine hypothetical data is used when executing test scripts.

System and Communications Protection (SC) – *Technical*

SC-1 – System and Communications Protection Policy and Procedures (High)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: SC-1; FISCAM: TAC-3.2.E.1; IRS-1075: 5.6.3.4#1, 5.6.3.4#2; NIST 800-53/53A: SC-1; PISP: 4.16.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and communications protection policy and procedures;
(ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and
(iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and communications protection responsibilities.

ASSESSMENT PROCEDURE: SC-1.2

Assessment Objective

Determine if:
(i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and communications protection responsibilities.

SC-2 – Application Partitioning (High)

Control

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Guidance

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Applicability: All	**References:** ARS: SC-2; NIST 800-53/53A: SC-2; PISP: 4.16.2	**Related Controls:**

ASSESSMENT PROCEDURE: SC-2.1

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Separation of user functionality from information system management functionality.

SC-2(CMS-1) – Enhancement (High)

Control

Place all CMS servers allowing public access within a DMZ environment, and disallow direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Applicability: All	**References:** ARS: SC-2(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-2(CMS-1).1

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Interview: Selected organizational personnel with network administration responsibilities to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Test: All CMS servers allowing public access to determine if the organization places these servers within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

SC-3 – Security Function Isolation (High)

Control

Information system security functions shall be isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system shall maintain a separate execution domain (e.g., address space) for each executing process.

Guidance

The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Applicability: All	**References:** ARS: SC-3; NIST 800-53/53A: SC-3; PISP: 4.16.3	**Related Controls:**

ASSESSMENT PROCEDURE: SC-3.1

Assessment Objective

Determine if:

(i) the organization defines the security functions of the information system to be isolated from nonsecurity functions; and

(ii) the information system isolates security functions from nonsecurity functions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Separation of security functions from nonsecurity functions within the information system.

SC-3(1) – Enhancement (High)

Control

Employ hardware separation mechanisms to facilitate the isolation of security functions.

Applicability: All	**References:** ARS: SC-3(1); NIST 800-53/53A: SC-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-3(1).1

Assessment Objective

Determine if the information system employs underlying hardware separation mechanisms to facilitate security function isolation.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; hardware separation mechanisms; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Hardware separation mechanisms facilitating security function isolation.(Optional)

SC-3(2) – Enhancement (High)

Control

Isolate critical security functions from both non-security functions and other security functions.

Applicability: All	**References:** ARS: SC-3(2); NIST 800-53/53A: SC-3(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-3(2).1

Assessment Objective

Determine if:
(i) the organization defines the critical security functions of the information system to be isolated from both nonsecurity functions and from other security functions; and
(ii) the information system isolates critical security functions from both nonsecurity functions and from other security functions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; list of critical security functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Isolation of critical security functions.(Optional)

SC-3(3) – Enhancement (High)

Control

Minimize the number of non-security functions included within the isolation boundary containing security functions.

Applicability: All	**References:** ARS: SC-3(3); NIST 800-53/53A: SC-3(3)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-3(3).1

Assessment Objective

Determine if the information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SC-3(4) – Enhancement (High)

Control

Implement security functions in largely independent modules that avoid unnecessary interactions between modules.

Applicability: All	**References:** ARS: SC-3(4); NIST 800-53/53A: SC-3(4)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-3(4).1

Assessment Objective

Determine if the information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SC-3(5) – Enhancement (High)

Control

Implement security functions in a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Applicability: All	**References:** ARS: SC-3(5); NIST 800-53/53A: SC-3(5)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-3(5).1

Assessment Objective

Determine if the information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SC-4 – Information Remnance (High)

Control

No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.

Guidance

Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

Applicability: All	**References:** ARS: SC-4; IRS-1075: 5.6.3.4#2, 5.6.3.4#3; NIST 800-53/53A: SC-4; PISP: 4.16.4	**Related Controls:**

ASSESSMENT PROCEDURE: SC-4.1

Assessment Objective

Determine if the information system prevents unauthorized and unintended information transfer via shared system resources.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for unauthorized and unintended transfer of information via shared system resources.

SC-4(0) – Enhancement (High)

Control

Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Ensure that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure.

Applicability: All	**References:** ARS: SC-4(0); IRS-1075: 5.6.3.4#2; NIST 800-53/53A: SC-4; PISP: 4.16.4	**Related Controls:**

ASSESSMENT PROCEDURE: SC-4(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for unauthorized and unintended transfer of information via shared system resources.

SC-4(PII-1) – Enhancement (High)

Control

For PII, when authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting PII from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

Applicability: All	**References:** IRS-1075: 3.3#2	**Related Controls:**

ASSESSMENT PROCEDURE: SC-4(PII-1).1

Assessment Objective

Determine if the organization determines authorizations for further disclosures (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting PII from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

Assessment Methods And Objects

Examine: Bulk record identities which have been transmitted externally to another organization to determine if the records contain:

- approximate number of personal records
- date of the transmission
- best possible description of the records

• the name of the individuals making/receiving the transmission.

SC-5 – Denial of Service Protection (High)

Control

Mechanisms shall be established to prevent, or limit the effects of well-known, detectable, and preventable denial-of-service attacks.

Guidance

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Applicability: All	**References:** ARS: SC-5; NIST 800-53/53A: SC-5; PISP: 4.16.5	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5.1

Assessment Objective

Determine if:
(i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and
(ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system for protection against or limitation of the effects of denial of service attacks.

SC-5(0) – Enhancement (High)

Control

Protect the information system against the denial-of-service attacks defined on the following sites or within the following documents:
- SANS Organization www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and
- NIST CVE List http://checklists.nist.gov/home.cfm.

Applicability: All	**References:** ARS: SC-5(0); NIST 800-53/53A: SC-5; PISP: 4.16.5	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan (for list of organization-defined types of denial of service attacks to protect against or limit); information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system for protection against or limitation of the effects of denial of service attacks.

SC-5(1) – Enhancement (High)

Control

Restrict the ability of users to launch denial of service attacks against other information systems or networks.

Applicability: All	**References:** ARS: SC-5(1); NIST 800-53/53A: SC-5(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5(1).1

Assessment Objective

Determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].(Optional)
Test: Information system for protection against or limitation of the effects of denial of service attacks].(Optional)

SC-5(2) – Enhancement (High)

Control

Maintain excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

Applicability: All	References: ARS: SC-5(2); NIST 800-53/53A: SC-5(2)	Related Controls:

ASSESSMENT PROCEDURE: SC-5(2).1

Assessment Objective

Determine if the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].(Optional)

SC-6 – Resource Priority (High)

Control

Mechanisms shall be implemented to provide for allocation of information system resources based upon priority. Priority protection shall ensure that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.

Applicability: All	References: ARS: SC-6; FISCAM: TSC-1.1; NIST 800-53/53A: SC-6; PISP: 4.16.6	Related Controls:

ASSESSMENT PROCEDURE: SC-6.1

Assessment Objective

Determine if the information system limits the use of resources by priority.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing prioritization of information system resources; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SC-7 – Boundary Protection (High)

Control

Automated boundary protection mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces. The operational failure of the boundary protection mechanisms shall not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing site shall provide the same levels of protection as those of the primary site.

Guidance

Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-77 provides guidance on virtual private networks.

Applicability: All	References: ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	Related Controls: AC-4, CA-3, MP-4, RA-2

ASSESSMENT PROCEDURE: SC-7.1

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design

documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Selected organizational personnel with boundary protection responsibilities.
Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system.

SC-7(1) – Enhancement (High)

Control

Physically allocate publicly-accessible information system components (e.g., public web servers, public email servers, public DNS servers) to separate sub-networks with separate physical network interfaces.

Guidance

Publicly accessible information system components include, for example, public web servers.

Applicability: All	**References:** ARS: SC-7(1); NIST 800-53/53A: SC-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(1).1

Assessment Objective

Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records.

SC-7(2) – Enhancement (High)

Control

Prevent public access into the internal networks except as appropriately mediated.

Applicability: All	**References:** ARS: SC-7(2); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(2).1

Assessment Objective

Determine if:
(i) the organization defines the mediation necessary for public access to the organization's internal networks; and
(ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing access controls for public access to the organization's internal networks.

SC-7(3) – Enhancement (High)

Control

Limit the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

Applicability: All	**References:** ARS: SC-7(3); NIST 800-53/53A: SC-7(3)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(3).1

Assessment Objective

Determine if the organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-7(4) – Enhancement (High)

Control

Maintain a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

Applicability: All	**References:** ARS: SC-7(4); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(4)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(4).1

Assessment Objective

Determine if:

(i) the organization defines the security controls (i.e., boundary protection devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service; and

(ii) the organization implements a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.

SC-7(5) – Enhancement (High)

Control

Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.

Applicability: All	**References:** ARS: SC-7(5); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(5)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(5).1

Assessment Objective

Determine if the information system denies network traffic by default and allows network traffic by exception.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.

SC-7(CMS-1) – Enhancement (High)

Control

Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Applicability: All	**References:** ARS: SC-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(CMS-1).1

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; and automated mechanisms implementing boundary protection capability within the information system to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

SC-7(CMS-2) – Enhancement (High)

Control

Utilize stateful inspection / application firewall hardware and software.

Applicability: All	**References:** ARS: SC-7(CMS-2); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(CMS-2).1

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and
(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; and automated mechanisms implementing boundary protection capability within the information system to determine if the organization utilizes stateful inspection / application firewall hardware and software.

SC-7(CMS-3) – Enhancement (High)

Control

Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Applicability: All	**References:** ARS: SC-7(CMS-3)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(CMS-3).1

Assessment Objective

Determine if the organization defines key internal boundaries of the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

SC-8 – Transmission Integrity (High)

Control

Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the integrity of CMS information while in transit.

Guidance

If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission integrity using IPSec. NIST SP 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Applicability: All	**References:** ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PISP: 4.16.8	**Related Controls:**

ASSESSMENT PROCEDURE: SC-8.1

Assessment Objective

Determine if the information system protects the integrity of transmitted information.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Transmission integrity capability within the information system.

SC-8(1) – Enhancement (High)

Control

Employ approved cryptographic mechanisms to ensure recognition of changes to information during transmission.

Guidance

Alternative physical protection measures include, for example, protected distribution systems.

Applicability: All	**References:** ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-8(1).1

Assessment Objective

Determine if the information system employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Cryptographic mechanisms implementing transmission integrity capability within the information system.

SC-8(CMS-1) – Enhancement (High)

Control

Employ appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13).

Applicability: All	**References:** ARS: SC-8(CMS-1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(c)(1), 164.312(e)(2)(i)	**Related Controls:** SC-13

ASSESSMENT PROCEDURE: SC-8(CMS-1).1

Assessment Objective

Determine if the information system protects the integrity of transmitted information.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization employs appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13).

Interview: Network administrators to determine if the organization employs appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13).

Test: Transmission integrity capability within the information system to determine if the organization employs appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13).

SC-9 – Transmission Confidentiality (High)

Control

Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the confidentiality of CMS sensitive information while in transit.

Guidance

If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission confidentiality using IPSec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Applicability: All	**References:** ARS: SC-9; HIPAA: 164.312(e)(1); IRS-1075: 5.6.3.4#2, 5.6.3.4#4.1; NIST 800-53/53A: SC-9; PISP: 4.16.9	**Related Controls:** AC-17

ASSESSMENT PROCEDURE: SC-9.1

Assessment Objective

Determine if the information system protects the confidentiality of transmitted information.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records.

Test: Transmission confidentiality capability within the information system.

SC-9(1) – Enhancement (High)

Control

Encryption is not required within a secured network. When transmitting data outside of a secured network:

(a) An approved encryption method must be used (see SC-13, Use of Cryptography, PISP 4.16.13) (see SC-CMS-4 for E-Mail), and
(b) Either a VPN or dedicated leased lines/circuits must be used.

Guidance

Alternative physical protection measures include, for example, protected distribution systems.

Applicability: All	**References:** ARS: SC-9(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(e)(1), 164.312(e)(2)(ii); IRS-1075: 5.6.3.4#2, 5.7#1; NIST 800-53/53A: SC-9(1)	**Related Controls:** SC-13

ASSESSMENT PROCEDURE: SC-9(1).1

Assessment Objective

Determine if the information system employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measure.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

Test: Cryptographic mechanisms implementing transmission confidentiality capability within the information system.

SC-9(PII-1) – Enhancement (High)

Control

When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Applicability: All	**References:** IRS-1075: 5.7.4#1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-9(PII-1).1

Assessment Objective

Determine if the organization sending and receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Assessment Methods And Objects

Examine: Fax machine locations for secure custodial coverage of outgoing and incoming PII transmitted data.

Test: Send or receive a simulated PII fax to ensure that:
(i) a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines is located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients is maintained; and (iii) a cover sheet is used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

SC-10 – Network Disconnect (High)

Control

Technical controls shall be established and implemented effectively to ensure that network connections are properly terminated at the end of user sessions, or upon the occurrence of specified conditions (e.g., a period of inactivity).

Guidance

The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Applicability: All	**References:** ARS: SC-10; NIST 800-53/53A: SC-10; PISP: 4.16.10	**Related Controls:**

ASSESSMENT PROCEDURE: SC-10.1

Assessment Objective

Determine if:
(i) the organization defines the time period of inactivity before the information system terminates a network connection; and
(ii) the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.

Test: Network disconnect capability within the information system.

SC-10(0) – Enhancement (High)

Control

Configure the information system to forcibly disconnect network connections at the end of a session, or after fifteen (15) minutes of inactivity, for mainframe sessions.

Applicability: All	**References:** ARS: SC-10(0); FISCAM: TAC-3.2.C.3; NIST 800-53/53A: SC-10; PISP: 4.16.10	**Related Controls:**

ASSESSMENT PROCEDURE: SC-10(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.

Test: Network disconnect capability within the information system.

SC-11 – Trusted Path (High)

Control

Technical controls shall be established and implemented effectively to provide the capability to establish trusted communications paths between authorized users and the security functionality of the information system.

Guidance

A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Applicability: All	**References:** ARS: SC-11; NIST 800-53/53A: SC-11; PISP: 4.16.11	**Related Controls:**

ASSESSMENT PROCEDURE: SC-11.1

Assessment Objective

Determine if:

(i) the organization defines the security functions within the information system that are included in a trusted communications path;

(ii) the organization-defined security functions include information system authentication and reauthentication; and

(iii) the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing trusted communications paths; information system security plan; information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing trusted communications paths within the information system.(Optional)

SC-11(0) – Enhancement (High)

Control

At a minimum, a trusted communications path is established between the user and the following system security functions: system authentication, re-authentication, and key management.

Applicability: All	**References:** ARS: SC-11(0); FISCAM: TAC-3.2.E.1; PISP: 4.16.11	**Related Controls:**

ASSESSMENT PROCEDURE: SC-11(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing trusted communications paths; information system security plan (for organization-defined security functions to include for authentication and reauthentication); information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records.

Test: Automated mechanisms implementing trusted communications paths within the information system.

SC-12 – Cryptographic Key Establishment and Management (High)

Control

When cryptography is required and used within the information system, documented procedures shall be implemented effectively for cryptographic key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect sensitive information shall be controlled and distributed using the NIST SP 800-56 and NIST SP 800-57 approved key management guidance.

Guidance

NIST SP 800-56 provides guidance on cryptographic key establishment. NIST SP 800-57 provides guidance on cryptographic key management.

Applicability: All	References: ARS: SC-12; IRS-1075: 5.7.1#1; NIST 800-53/53A: SC-12; PISP: 4.16.12	Related Controls:

ASSESSMENT PROCEDURE: SC-12.1

Assessment Objective

Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with responsibilities for cryptographic key establishment or management.

Test: Automated mechanisms implementing cryptographic key management and establishment within the information system.

SC-12(CMS-1) – Enhancement (High)

Control

Employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall prohibit the use of encryption keys that are not recoverable by authorized personnel, require senior management approval to authorize recovery of keys by other than the key owner, and comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Applicability: All	References: ARS: SC-12(CMS-1)	Related Controls: MA-CMS-1, MA-CMS-2, SC-13

ASSESSMENT PROCEDURE: SC-12(CMS-1).1

Assessment Objective

Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Interview: A sample of organizational personnel with responsibilities for cryptographic key establishment or management to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Test: Automated mechanisms implementing cryptographic key management and establishment within the information system to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

SC-13 – Use of Cryptography (High)

Control

When cryptographic mechanisms are used, procedures shall be developed, documented, and implemented effectively to ensure they comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. All such mechanisms shall be FIPS 140-2 (as amended and revised) compliant and NIST validated.

Guidance

The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	References: ARS: SC-13; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2, 5.6.3.4#4.2-3; NIST 800-53/53A: SC-13; PISP: 4.16.13	Related Controls: AC-17(CMS-1), AC-19(CMS-1), AC-3, AC-3(CMS-1), MP-4(PII-1), SC-12(CMS-1), SC-8(CMS-1), SC-9(1)

ASSESSMENT PROCEDURE: SC-13.1

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

SC-14 – Public Access Protections (High)

Control

Technical controls shall be developed, documented, and implemented effectively to protect the integrity of the publicly accessible CMS information and applications.

Guidance

CMS refers to the National Institute of Standards and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix A provides a summary for remote access controls.

Applicability: All	**References:** ARS: SC-14; NIST 800-53/53A: SC-14; PISP: 4.16.14	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14.1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing access controls and boundary protection for publicly available information and applications within the information system.

SC-14(CMS-1) – Enhancement (High)

Control

Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

Applicability: All	**References:** ARS: SC-14(CMS-1); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14(CMS-1).1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

Interview: Organizational personnel to determine if network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

Test: Interfaces for all public-facing networks to determine if network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

SC-14(CMS-2) – Enhancement (High)

Control

If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.

Applicability: All	**References:** ARS: SC-14(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14(CMS-2).1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information

system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.

Interview: MA owners for each public-facing MA to determine if e-authentication is required and implemented in conjunction with or related to public access protections; refer to ARS Appendix A for e-Authentication Standards.

Test: All public-facing systems to determine if e-authentication is required and implemented in conjunction with or related to public access protections; refer to ARS Appendix A for e-Authentication Standards.

SC-15 – Collaborative Computing (High)

Control

Running collaborative computing mechanisms on CMS information systems shall require authorization by the CIO or his/her designated representative. The authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used. Collaborative computing mechanisms shall not be activated remotely.

Guidance

Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

Applicability: All	**References:** ARS: SC-15; NIST 800-53/53A: SC-15; PISP: 4.16.15	**Related Controls:**

ASSESSMENT PROCEDURE: SC-15.1

Assessment Objective

Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users.

SC-15(1) – Enhancement (High)

Control

If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:
Provide physical disconnect of cameras or microphones in a manner that supports ease of use.

Applicability: All	**References:** ARS: SC-15(1); NIST 800-53/53A: SC-15(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-15(1).1

Assessment Objective

Determine if the information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Physical disconnect of collaborative computing devices.(Optional)

SC-15(CMS-1) – Enhancement (High)

Control

If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:
Ensure the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

Applicability: All	**References:** ARS: SC-15(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-15(CMS-1).1

Assessment Objective

Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and

(b) Explicit indication to the local user of the fact that it is in use.
Interview: Personnel to determine if the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.
Test: Automated mechanisms implementing access controls for collaborative computing environments and alert notification for local users to determine if the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

SC-16 – Transmission of Security Parameters (High)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure that CMS information systems reliably associate security parameters with information exchanged between information systems.

Guidance

Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Applicability: All	**References:** ARS: SC-16; NIST 800-53/53A: SC-16; PISP: 4.16.16	**Related Controls:**

ASSESSMENT PROCEDURE: SC-16.1

Assessment Objective

Determine if the information system reliably associates security parameters with information exchanged between information systems.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission of security parameters; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Automated mechanisms supporting reliable transmission of security parameters between information systems.(Optional)

SC-17 – Public Key Infrastructure Certificates (High)

Control

All public key certificates used within the CMS information system shall be issued in accordance with a defined certification policy and certification practice statement. Registration to receive a public key certificate shall include authorization by a supervisor or a responsible official, and shall be done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

Guidance

For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24. NIST SP 800-32 provides guidance on public key technology. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**References:** ARS: SC-17; NIST 800-53/53A: SC-17; PISP: 4.16.17	**Related Controls:**

ASSESSMENT PROCEDURE: SC-17.1

Assessment Objective

Determine if the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; NIST SP 800-32; other relevant documents or records.
Interview: Organizational personnel with public key infrastructure certificate issuing responsibilities.

SC-18 – Mobile Code (High)

Control

CMS shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause harm to CMS information systems. The organization shall document, monitor, and implement controls for the use of mobile code within the CMS information system. Appropriate officials shall authorize or deny the use of mobile code. The organization shall implement controls and procedures for mobile code in accordance with NIST SP 800-28.

Guidance

Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the

development, acquisition, or introduction of unacceptable mobile code within the information system. NIST SP 800-28 provides guidance on active content and mobile code.

Applicability: All	References: ARS: SC-18; NIST 800-53/53A: SC-18; PISP: 4.16.18	Related Controls:

ASSESSMENT PROCEDURE: SC-18.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and
(ii) the organization authorizes, monitors, and controls the use of mobile code within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation guidance; NIST SP 800-28; other relevant documents or records.
Interview: Organizational personnel with mobile code authorization, monitoring, and control responsibilities.
Test: Mobile code authorization and monitoring capability for the organization.

SC-19 – Voice Over Internet Protocol (High)

Control

CMS shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to harm CMS information systems. The organization shall document, monitor, and implement controls for the use of VoIP within a CMS information system. When VoIP is implemented, the organization shall adhere to the NIST SP 800-58 guidance.

Guidance

NIST SP 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.

Applicability: All	References: ARS: SC-19; NIST 800-53/53A: SC-19; PISP: 4.16.19	Related Controls:

ASSESSMENT PROCEDURE: SC-19.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and
(ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other relevant documents or records.
Interview: Organizational personnel with VoIP authorization and monitoring responsibilities.

SC-19(CMS-1) – Enhancement (High)

Control

The use of VoIP must be authorized in writing by the CMS CIO, or his/her designated representative.

Applicability: All	References: ARS: SC-19(CMS-1)	Related Controls:

ASSESSMENT PROCEDURE: SC-19(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and
(ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; and other relevant documents or records to determine if the use of VoIP is authorized in writing by the CMS CIO, or his/her designated representative.
Interview: Organizational personnel with VoIP authorization and monitoring responsibilities to determine if the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

SC-20 – Secure Name / Address Resolution Service (Authoritative Source) (High)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

Guidance

This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment.

Applicability: All	**References:** ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20	**Related Controls:**

ASSESSMENT PROCEDURE: SC-20.1

Assessment Objective

Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); NIST SP 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing secure name/address resolution service (authoritative source) within the information system.

SC-20(1) – Enhancement (High)

Control

When the information system is operating as part of a distributed, hierarchical namespace, ensure that it provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

Guidance

An example means to indicate the security status of child subspaces is through the use of delegation signer resource records.

Applicability: All	**References:** ARS: SC-20(1); NIST 800-53/53A: SC-20(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-20(1).1

Assessment Objective

Determine if the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services within the information system.(Optional)

SC-21 – Secure Name / Address Resolution Service (Recursive or Caching Resolver) (High)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

Guidance

A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST SP 800-81 provides guidance on secure domain name system deployment.

Applicability: All	**References:** ARS: SC-21; NIST 800-53/53A: SC-21; PISP: 4.16.21	**Related Controls:**

ASSESSMENT PROCEDURE: SC-21.1

Assessment Objective

Determine if the information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing data origin authentication and integrity verification for resolution services within the information system.

SC-22 – Architecture and Provisioning for Name / Address Resolution Service (High)

Control

Information systems that collectively provide name / address resolution service for an organization shall be fault tolerant and implement role separation.

Guidance

A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified. NIST SP 800-81 provides guidance on secure DNS deployment.

Applicability: All	**References:** ARS: SC-22; NIST 800-53/53A: SC-22; PISP: 4.16.22	**Related Controls:**

ASSESSMENT PROCEDURE: SC-22.1

Assessment Objective

Determine if the information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; NIST SP 800-81; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms supporting name/address resolution service for fault tolerance and role separation.

SC-23 – Session Authenticity (High)

Control

Technical controls shall be developed, documented, and effectively implemented to ensure that CMS information systems provide mechanisms to protect the authenticity of communications sessions.

Guidance

This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST SP 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST SP 800-77 provides guidance on the deployment of IPSec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST SP 800-95 provides guidance on secure web services.

Applicability: All	**References:** ARS: SC-23; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-23; PISP: 4.16.23	**Related Controls:**

ASSESSMENT PROCEDURE: SC-23.1

Assessment Objective

Determine if the information system provides mechanisms to protect the authenticity of communications sessions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing session authenticity; NIST SP 800-52, 800-77, and 800-95; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing session authenticity.

SC-CMS-1 – Desktop Modems (High)

Control

Users are prohibited from installing desktop modems.

Guidance

Desktop Modems allow backdoors into the network putting the CMS data and network at very high risk.

Applicability: All	**References:** ARS: SC-CMS-1; PISP: 4.16.24	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-1.1

Assessment Objective

Determine if the organization has implement a policy which assists in prohibiting the installation of unauthorized desktop modems.

Assessment Methods And Objects

Examine: Organizational policy does not allow unauthorized desktop modems.

SC-CMS-2 – Identify and Detect Unauthorized Modems (High)

Control

Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized modems.

Guidance

It is good practice that management approve any automated tool or utility for checking for unauthorized modems.

Applicability: All	**References:** ARS: SC-CMS-2; PISP: 4.16.25	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-2.1

Assessment Objective

Determine if the organization has an approved automated system to test for unauthorized modems.

Assessment Methods And Objects

Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

SC-CMS-2(CMS-0) – Enhancement (High)

Control

Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly.

Applicability: All	**References:** ARS: SC-CMS-2(CMS-0)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less than quarterly.

SC-CMS-3 – Secondary Authentication and Encryption (High)

Control

Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network.

Guidance

A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP.

Applicability: All	**References:** ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-3.1

Assessment Objective

Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit.

Assessment Methods And Objects

Examine: In-transit technical controls implement and documents for sensitive information outside the secure network.

SC-CMS-3(CMS-0) – Enhancement (High)

Control

Enable and force use of application security mechanisms, such as Transport Layer Security (TLS). Utilize CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).

Applicability: All	References: ARS: SC-CMS-3(CMS-0)	Related Controls:

ASSESSMENT PROCEDURE: SC-CMS-3(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Documentation to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization utilizes CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).

Interview: Organizational personnel to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization utilizes CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).

Test: Information system to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization utilizes CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).

SC-CMS-3(CMS-1) – Enhancement (High)

Control

If e-authentication is required and implemented, refer to ARS Appendix A for e-Authentication Standards controls and procedures.

Applicability: All	References: ARS: SC-CMS-3(CMS-1)	Related Controls:

ASSESSMENT PROCEDURE: SC-CMS-3(CMS-1).1

Assessment Objective

Determine if the organization that uses e-authentication is required to refer to ARS Appendix A for e-Authentication Standards controls and procedures.

Assessment Methods And Objects

Examine: Network documentation to determine which recommends enabling application security mechanisms, such as TLS, and utilizing minimum encryption and password authentication although, no specific requirements are mandatory.

Interview: Organizational personnel to determine if enabling application security mechanisms is recommended, such as TLS, and utilizing minimum encryption and password authentication although, no specific requirements are mandatory.

Test: Information system to determine if application security mechanisms are enabled, such as TLS, and the organization utilizes minimum encryption and password authentication although, no specific requirements are mandatory.

SC-CMS-4 – Electronic Mail (High)

Control

Controls shall be developed, documented, and implemented effectively to protect CMS sensitive information that is sent via e-mail.

Guidance

A good place to obtain technical controls for handling sensitive information via e-mail is the NIST SP.

Applicability: All	References: ARS: SC-CMS-4; PISP: 4.16.27	Related Controls:

ASSESSMENT PROCEDURE: SC-CMS-4.1

Assessment Objective

Determine if the organization effectively develops, documents, and implements protections for CMS sensitive information that is sent via e-mail.

Assessment Methods And Objects

Examine: Documentation to determine if all e-mail messages with CMS sensitive information are transmitted using protective measures.

Interview: Organizational personnel to determine if all e-mail messages with CMS sensitive information is protected, controlled, and monitored.

SC-CMS-4(CMS-0) – Enhancement (High)

Control

Prior to sending an email, place all CMS sensitive information in an encrypted attachment.

Applicability: All	References: ARS: SC-CMS-4(CMS-0); IRS-1075: 5.7.3#1	Related Controls:

ASSESSMENT PROCEDURE: SC-CMS-4(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Documentation to determine if all e-mail messages are encrypted and verify encryption / decryption for received messages.

Interview: Organizational personnel to determine if all e-mail messages are encrypted, and encryption /decryption for received messages.

SC-CMS-5 – Persistent Cookies (High)

Control

The use of persistent cookies on a CMS web site is prohibited unless explicitly approved in writing by the DHHS Secretary.

Guidance

Requests to DHHS should be via CMS.

Applicability: All	**References:** ARS: SC-CMS-5; PISP: 4.16.28	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-5.1

Assessment Objective

Determine if the organization does not use a persistent cookie configuration on a CMS web site to remember subsequent visits unless approved in writing by the DHHS Secretary.

Assessment Methods And Objects

Examine: CMS web site baseline and change management documentation for configurations using persistent cookies.

Interview: Web site administrators to determine if the CMS web site has persistent cookies enable in the baseline configuration or have written approval to enable persistent cookies from the DHHS Secretary.

SC-CMS-6 – Network Interconnection (High)

Control

Controls shall be developed, documented, and implemented effectively to ensure that only properly authorized network interconnections external to the system boundaries are established.

Guidance

A good place to obtain technical controls for securing interconnections external to the system boundaries is the NIST SP.

Applicability: All	**References:** ARS: SC-CMS-6; PISP: 4.16.29	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-6.1

Assessment Objective

Determine if the organization effectively documents and implements authorized network interconnections external to the system boundaries.

Assessment Methods And Objects

Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards for all external interconnections.

SC-CMS-6(CMS-0) – Enhancement (High)

Control

Ensure remote location(s) (e.g., users and sites using a network interconnection external to the system boundaries) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

Applicability: All	**References:** ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

Interview: Personnel to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

System and Information Integrity (SI) – *Operational*

SI-1 – System and Information Integrity Policy and Procedures (High)

Control

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems, software, and information. The procedures and automated mechanisms shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. It is good practice to have an automated system which is host based to automatically detect, block/filter and alert supervisors or managers that possible unauthorized changes to software and the information system have occurred.

Applicability: All	**References:** ARS: SI-1; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-1; PISP: 4.17.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and information integrity policy and procedures;
(ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and information integrity policy and procedures; and
(iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and information integrity responsibilities.

ASSESSMENT PROCEDURE: SI-1.2

Assessment Objective

Determine if:
(i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and information integrity responsibilities.

SI-2 – Flaw Remediation (High)

Control

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. The flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

Guidance

The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. It is a good practice to test the changes in a laboratory environment on like systems prior to approving and implementing the updates and changes. NIST SP 800-40, provides guidance on security patch installation and patch management.

Applicability: All	**References:** ARS: SI-2; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2; PISP: 4.17.2	**Related Controls:** CA-2, CA-4, CA-7, CM-3, IR-4, SI-11

ASSESSMENT PROCEDURE: SI-2.1

Assessment Objective

Determine if:
(i) the organization identifies, reports, and corrects information system flaws;
(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;
(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;
(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and
(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(0) – Enhancement (High)

Control

Correct identified information system flaws on production equipment within 72 hours.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and
(b) Manage the flaw remediation process centrally.

Applicability: All	**References:** ARS: SI-2(0); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2; PISP: 4.17.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(1) – Enhancement (High)

Control

Updates are installed automatically.

Applicability: All	**References:** ARS: SI-2(1); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-2(1).1

Assessment Objective

Determine if the organization centrally manages the flaw remediation process and installs updates automatically.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records.

Test: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates.

SI-2(2) – Enhancement (High)

Control

Employ automated mechanisms periodically and upon demand to determine the state of information system components with regard to flaw remediation.

Applicability: All	**References:** ARS: SI-2(2); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-	**Related Controls:**

	2(2)	

ASSESSMENT PROCEDURE: SI-2(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system flaw remediation update status.

SI-3 – Malicious Code Protection (High)

Control

Automated malicious code protection mechanisms that include a capability of automatic updates shall be in place and supporting procedures shall be developed, documented, and implemented effectively to identify and isolate suspected malicious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical information system entry points, and at each workstation, server, or mobile computing device on the network to detect and eradicate malicious code transported by email, email attachments, removable media or other methods. Business owners shall use antiviral software products from multiple vendors, if possible, and update virus protection mechanisms whenever new releases are available.

Guidance

The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST SP 800-83 provides guidance on implementing malicious code protection.

Applicability: All	**References:** ARS: SI-3; FISCAM: TCC-1.3.2; IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3.1

Assessment Objective

Determine if:

(i) the information system implements malicious code protection;

(ii) the organization employs malicious code protection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;

(iii) the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities;

(iv) the organization updates malicious code protection mechanisms whenever new releases are available; and

(v) the malicious code protection mechanisms are appropriately updated to include the latest malicious code definitions, configured to perform periodic scans of the information system as well as real-time scans of files from external sources as the files are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(0) – Enhancement (High)

Control

Implement malicious code protection at information system entry points, including firewalls, email servers, remote access servers, workstations, servers, and mobile computing devices by employing automated mechanisms to detect and eradicate malicious code transported by email, email attachments, and removable media.

Applicability: All	**References:** ARS: SI-3(0); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(1) – Enhancement (High)

Control

Manage and update malicious code protection software centrally with automatic updates for the latest malicious code definitions whenever new releases are available.

Applicability: All	**References:** ARS: SI-3(1); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(1).1

Assessment Objective

Determine if the organization centrally manages malicious code protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(2) – Enhancement (High)

Control

Employ automated mechanisms to update malicious code protection.

Applicability: All	**References:** ARS: SI-3(2); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(2).1

Assessment Objective

Determine if the organization automatically updates malicious code protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automatic update capability for malicious code protection.

SI-3(CMS-1) – Enhancement (High)

Control

Enable real-time file scanning. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and every twelve (12) hours.

Applicability: All	**References:** ARS: SI-3(CMS-1); IRS-1075: 5.6.2.5#1.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(CMS-1).1

Assessment Objective

Determine if:
(i) real-time file scanning is enabled;
(ii) real-time desktop malicious code scanning is enabled and monitored; and
(iii) software is configured to perform critical system file scans during system boot and every twelve (12) hours.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records to determine real-time file scanning is enabled. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and every twelve (12) hours.

Interview: Personnel with system and information integrity responsibilities to determine real-time file scanning is enabled, desktop malicious code scanning software is installed, real-time protection, and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and every twelve (12) hours.

Test: Information system real-time file scanning is enabled, desktop malicious code scanning software is installed, real-time protection, and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and every twelve (12) hours.

SI-4 – Information System Monitoring Tools and Techniques (High)

Control

Effective monitoring tools and techniques providing real-time identification of unauthorized use, misuse, and abuse of the information system shall be implemented.

Guidance

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST SP 800-61 provides guidance on detecting attacks through various types of security technologies. NIST SP 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST SP 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST SP 800-94 provides guidance on intrusion detection and prevention.

Applicability: All	**References:** ARS: SI-4; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4; PISP: 4.17.4	**Related Controls:** AC-8, AU-4, CM-6

ASSESSMENT PROCEDURE: SI-4.1

Assessment Objective

Determine if the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

SI-4(1) – Enhancement (High)

Control

Connect individual IDS devices to a common IDS management network using common protocols.

Applicability: All	**References:** ARS: SI-4(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(1).1

Assessment Objective

Determine if the organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.(Optional)

Test: Information system-wide intrusion detection capability.(Optional)

SI-4(2) – Enhancement (High)

Control

Employ automated information system monitoring tools to support near-real-time analysis of events.

Applicability: All	**References:** ARS: SI-4(2); NIST 800-53/53A: SI-4(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(2).1

Assessment Objective

Determine if the organization employs automated tools to support near-real-time analysis of events.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records.

Test: Automated tools supporting near real-time event analysis.

SI-4(3) – Enhancement (High)

Control

Employ automated tools to integrate intrusion detection tools into access control mechanisms to enable rapid response to attacks through the re-configuration of IDS settings to support attack isolation and elimination.

Applicability: All	**References:** ARS: SI-4(3); NIST 800-53/53A: SI-4(3)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(3).1

Assessment Objective

Determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.(Optional)

Test: Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms.(Optional)

SI-4(4) – Enhancement (High)

Control

Monitor inbound and outbound communications for unusual or unauthorized activities or conditions.

Guidance

Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.

Applicability: All	**References:** ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(4).1

Assessment Objective

Determine if:
(i) the organization identifies the types of activities or conditions considered unusual or unauthorized; and
(ii) the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; types of activities or conditions considered unusual or unauthorized; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system monitoring capability for inbound and outbound communications.

SI-4(5) – Enhancement (High)

Control

Real-time alerts are provided when indications of the following types of compromise, or potential compromise, occur:
(a) Presence of malicious code,
(b) Unauthorized export of information,
(c) Signaling to an external information system, or
(d) Potential intrusions.

Applicability: All	**References:** ARS: SI-4(5); NIST 800-53/53A: SI-4(5)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(5).1

Assessment Objective

Determine if:
(i) the organization identifies indications of compromise or potential compromise to the security of the information system; and
(ii) the information system provides a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system monitoring real-time alert capability.

SI-4(CMS-1) – Enhancement (High)

Control

Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.

Applicability: All	**References:** ARS: SI-4(CMS-1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(CMS-1).1

Assessment Objective

Determine if:
(i) IDS devices are installed at network perimeter points; and
(ii) host-based IDS sensors are installed on critical servers.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

Interview: Personnel with system and information integrity responsibilities to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

Test: Information system-wide intrusion detection capability to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

SI-5 – Security Alerts and Advisories (High)

Control

Procedures shall be developed, documented, and implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis, and for issuing IS alerts and advisories to appropriate personnel. Upon receipt of such alerts and advisories, personnel shall take appropriate response actions. The types of actions to be taken in response to security alerts / advisories shall be documented.

Guidance

The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST SP 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Applicability: All	**References:** ARS: SI-5; NIST 800-53/53A: SI-5; PISP: 4.17.5	**Related Controls:**

ASSESSMENT PROCEDURE: SI-5.1

Assessment Objective

Determine if:
(i) the organization receives information system security alerts/advisories on a regular basis;
(ii) the organization issues security alerts/advisories to appropriate organizational personnel; and
(iii) the organization takes appropriate actions in response to security alerts/advisories.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; NIST SP 800-40; records of security alerts and advisories; other relevant documents or records.

Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system.

SI-5(1) – Enhancement (High)

Control

Employ automated mechanisms to make security alerts and advisory information available to all appropriate personnel.

Applicability: All	**References:** ARS: SI-5(1); NIST 800-53/53A: SI-5(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-5(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records.

Test: Automated mechanisms implementing the distribution of security alert and advisory information.

SI-6 – Security Functionality Verification (High)

Control

Automated mechanisms shall be established and implemented effectively to provide the capability for CMS information systems to verify the correct operation of security functions on a regular basis,

and automatically to take appropriate response actions when security-related anomalies are discovered.

Guidance

The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Applicability: All	**References:** ARS: SI-6; NIST 800-53/53A: SI-6; PISP: 4.17.6	**Related Controls:**

ASSESSMENT PROCEDURE: SI-6.1

Assessment Objective

Determine if:
(i) the organization defines the appropriate conditions for conducting security function verification;
(ii) the organization defines, for periodic security function verification, the frequency of the verifications;
(iii) the organization defines information system responses to anomalies discovered during security function verification;
(iv) the information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification); and
(v) the information system responds to security function anomalies in accordance with organization-defined responses.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.
Test: Security function verification capability.

SI-6(0) – Enhancement (High)

Control

Configure the information system to automatically verify the correct operation of system security functions upon system startup and restart, upon command by users with appropriate access, and at least on a monthly routine basis and to notify system administration upon detection of security anomalies.

Applicability: All	**References:** ARS: SI-6(0); NIST 800-53/53A: SI-6; PISP: 4.17.6	**Related Controls:**

ASSESSMENT PROCEDURE: SI-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan (for organization-defined conditions for conducting security function verification, organization-defined frequency of security function verifications (if periodic), and organization-defined information system responses to security function anomalies); information system configuration settings and associated documentation; other relevant documents or records.
Test: Security function verification capability.

SI-6(1) – Enhancement (High)

Control

Employ automated mechanisms to provide centralized notification of failed automated security tests.

Applicability: All	**References:** ARS: SI-6(1); NIST 800-53/53A: SI-6(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-6(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to provide notification of failed security tests.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Automated mechanisms implementing alerts and/or notifications for failed automated security tests.(Optional)

SI-6(2) – Enhancement (High)

Control

Employ automated mechanisms to support centralized management of distributed security testing.

Applicability: All	**References:** ARS: SI-6(2); NIST 800-53/53A: SI-6(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-6(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to support management of distributed security testing.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Automated mechanisms supporting the management of distributed security function testing.(Optional)

SI-7 – Software and Information Integrity (High)

Control

Automated mechanisms for software and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to software. Good software engineering practices consistent with CMS IS policy and procedures shall be employed with regard to commercial-off-the-shelf (COTS) integrity mechanisms, and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications.

Guidance

The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Applicability: All	**References:** ARS: SI-7; FISCAM: TAN-3.1.2, TAN-3.2.1, TAN-3.2.2, TAY-2.1.4, TAY-2.2.2, TCP-2.1.2, TCP-2.1.3, TCP-2.1.4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7; PISP: 4.17.7	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7.1

Assessment Objective

Determine if:

(i) the information system detects and protects against unauthorized changes to software and information; and

(ii) the organization employs effective integrity verification tools in accordance with good software engineering practices.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records.

Test: Software integrity protection and verification capability.

SI-7(0) – Enhancement (High)

Control

Employ off-the-shelf integrity mechanisms such as parity checks, check-sums, error detection data validation techniques, cyclical redundancy checks, and cryptographic hashes to detect and protect against information tampering, errors, omissions and unauthorized changes to software and use tools to automatically monitor the integrity of the information system and the application it hosts.

Applicability: All	**References:** ARS: SI-7(0); FISCAM: TAC-3.3; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7; PISP: 4.17.7	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records.

Test: Software integrity protection and verification capability.

SI-7(1) – Enhancement (High)

Control

Perform weekly integrity scans of the system.

Applicability: All	**References:** ARS: SI-7(1); HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(1).1

Assessment Objective

Determine if:
(i) the organization defines the frequency of integrity scans on the information system; and
(ii) the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records.

SI-7(2) – Enhancement (High)

Control

Employ automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.

Applicability: All	**References:** ARS: SI-7(2); HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(2).1

Assessment Objective

Determine if the organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records.

SI-7(FIS-1) – Enhancement (High)

Control

A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing. Live data are not used in testing of program changes except to build test data files.

Applicability: All	**References:** FISCAM: TCC-2.1.6, TCC-2.1.7	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-1).1

Assessment Objective

Determine if:
(i) the organization provides a comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.
(ii) the organizational validation does not use live data in testing of program changes except to build test data files.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Test transactions and data.
Interview: Programmers, auditors, and quality assurance personnel.

SI-7(FIS-2) – Enhancement (High)

Control

User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.

Applicability: All; Optional for CWF, DC, EDC, SS	**References:** FISCAM: TCP-1.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-2).1

Assessment Objective

Determine if the organizational user-prepared record count and control totals documents help determine the completeness of data entry and processing.

Assessment Methods And Objects

Examine: Activity for developing record counts and control totals.
Examine: Application documentation.
Examine: Pertinent policies and procedures.
Interview: User management and personnel.

SI-7(FIS-3) – Enhancement (High)		
Control For on-line or real-time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing.		
Applicability: All; Optional for CWF	**References:** FISCAM: TCP-1.1.2	**Related Controls:**
ASSESSMENT PROCEDURE: SI-7(FIS-3).1		
Assessment Objective Determine if the organizational on-line or real-time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Pertinent policies and procedures. **Examine:** Supporting documentation generated by system. **Interview:** Application programmer, if available. **Interview:** User management and personnel.		
SI-7(FIS-4) – Enhancement (High)		
Control Record counts and control totals are established over and entered with transaction data, and reconciled to determine the completeness of data entry.		
Applicability: All	**References:** FISCAM: TCP-2.1.1	**Related Controls:**
ASSESSMENT PROCEDURE: SI-7(FIS-4).1		
Assessment Objective Determine if the organizational record counts and control totals are established over and entered with transaction data, and reconciled to determine the completeness of data entry. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Pertinent policies and procedures. **Examine:** Reconciliation activities. **Interview:** Data control personnel. **Interview:** User management and personnel.		
SI-7(FIS-5) – Enhancement (High)		
Control Reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated.		
Applicability: All	**References:** FISCAM: TCP-2.2.1	**Related Controls:**
ASSESSMENT PROCEDURE: SI-7(FIS-5).1		
Assessment Objective Determine if the organizational reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Pertinent policies and procedures. **Examine:** Reconciliation activities. **Interview:** Data control personnel. **Interview:** User management and personnel.		
SI-8 – Spam Protection (High)		
Control Automated mechanisms for spam protection shall be in place at critical information system entry points, workstations, servers, and mobile computing devices on the network. Supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect spam.		

Guidance

The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST SP 800-45 provides guidance on electronic mail security.

Applicability: All	**References:** ARS: SI-8; HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8; PISP: 4.17.8	**Related Controls:**

ASSESSMENT PROCEDURE: SI-8.1

Assessment Objective

Determine if:
(i) the information system implements spam protection;
(ii) the organization employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network;
(iii) the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail; and
(iv) the organization updates spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.
Test: Spam detection and handling capability.

SI-8(1) – Enhancement (High)

Control

Centrally manage spam protection mechanisms.

Applicability: All	**References:** ARS: SI-8(1); HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-8(1).1

Assessment Objective

Determine if the organization centrally manages spam protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

SI-8(2) – Enhancement (High)

Control

Automatically update spam protection mechanisms.

Applicability: All	**References:** ARS: SI-8(2); HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-8(2).1

Assessment Objective

Determine if the information system automatically updates spam protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Automatic update capability for spam protection.(Optional)

SI-9 – Information Input Restrictions (High)

Control

Automated mechanisms shall be in place to restrict information input to the information system to authorized personnel. Personnel authorized to input information to the information system shall be restricted beyond the typical access controls employed by the system, including limitations based on specific operational / project responsibilities.

Guidance

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Applicability: All	**References:** ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.1; NIST 800-53/53A: SI-9; PISP: 4.17.9	**Related Controls:**

ASSESSMENT PROCEDURE: SI-9.1

Assessment Objective

Determine if the organization restricts the capability to input information to the information system to authorized personnel.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SI-10 – Information Accuracy, Completeness, Validity, and Authenticity (High)

Control

Automated mechanisms shall verify information for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

Guidance

Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Applicability: All	**References:** ARS: SI-10; FISCAM: TAN-3.1.1, TAY-1.2.1, TAY-1.4.1, TAY-2.1.3, TCP-2.1.2, TCP-2.1.3, TCP-2.1.4; IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-10; PISP: 4.17.10	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10.1

Assessment Objective

Determine if:

(i) the information system checks information for accuracy, completeness, validity, and authenticity;

(ii) checks for accuracy, completeness, validity, and authenticity of information is accomplished as close to the point of origin as possible;

(iii) the information system employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions for format and content; and

(iv) the information system prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system capability for checking information for accuracy, completeness, validity, and authenticity.

SI-10(CMS-1) – Enhancement (High)

Control

Implement automated system checks of information for accuracy, completeness, validity, and authenticity.

Applicability: All	**References:** ARS: SI-10(CMS-1); FISCAM: TAN-3.1.1, TCP-2.1.3, TCP-2.1.4; IRS-1075: 5.6.2.5#1.1-2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(CMS-1).1

Assessment Objective

Determine if the information system checks information for accuracy, completeness, validity, and authenticity.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine that automated system checks of information for accuracy, completeness, validity, and authenticity are performed.

Interview: Personnel with system and information integrity responsibilities to determine that automated system checks of information for accuracy, completeness, validity, and authenticity are performed.

Test: Information system to determine that automated system checks of information for accuracy, completeness, validity, and authenticity are performed.

SI-10(FIS-1) – Enhancement (High)

Control

The source document is well-designed to aid the preparer and facilitate data entry and includes document pre-numbering and preprinting of transaction type and data field codes. The document

numbers, transaction types and field codes are entered into the system to facilitate completeness and sequence checking. Access to blank source documents is restricted to authorized personnel.

Applicability: All	**References:** FISCAM: TAN-1.1.1, TAN-1.1.2, TAN-1.1.3, TAY-1.1.1, TAY-1.1.2, TCP-1.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-1).1

Assessment Objective

Determine if the organizational source document is well-designed to aid the preparer and facilitate data entry and includes document pre-numbering and preprinting of transaction type and data field codes. The document numbers, transaction types and field codes are entered into the system to facilitate completeness and sequence checking. Access to blank source documents is restricted to authorized personnel.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Blank document storage area.
Examine: Procedures for recording and tracking of numbers if pre-numbered documents are used.
Examine: Source documents and data entry activities.
Interview: User management and personnel.

SI-10(FIS-2) – Enhancement (High)

Control

For batch application systems, a batch control sheet is prepared for a group of source documents, and includes: date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.

Applicability: All; Optional for CWF, SS	**References:** FISCAM: TAN-1.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-2).1

Assessment Objective

Determine if the organizational batch application systems prepared a batch control sheet for a group of source documents, and includes: date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Batch control sheets if batch application.
Examine: Prepared source documents and batches if batch application.
Interview: Users responsible for preparing batch control sheets and submitting the batch.

SI-10(FIS-3) – Enhancement (High)

Control

Key source documents require authorizing signatures. Data control unit personnel: verify that source documents are properly prepared and authorized; and monitor data entry and processing of source documents.

Applicability: All; Optional for CWF, SS	**References:** FISCAM: TAN-1.2.1, TAN-1.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-3).1

Assessment Objective

Determine if the organizational key source documents require authorizing signatures. Data control unit personnel: verify that source documents are properly prepared and authorized; and monitor data entry and processing of source documents.

Assessment Methods And Objects

Examine: Key source documents and data entry activities.
Examine: Pertinent policies and procedures.
Interview: Management and data control unit personnel.

SI-10(FIS-4) – Enhancement (High)

Control

Supervisory or control unit personnel review data and enter an authorizing code before data is released for processing.

Applicability: All	**References:** FISCAM: TAN-1.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-4).1

Assessment Objective

Determine if the organizational supervisory or control unit personnel review data and enter an authorizing code before data is released for processing.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Review process.
Interview: Management and data control unit personnel.

SI-10(FIS-5) – Enhancement (High)

Control

Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.

Applicability: All; Optional for CWF	**References:** FISCAM: TAY-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-5).1

Assessment Objective

Determine if the organization information system override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.

Assessment Methods And Objects

Examine: Application documentation.
Examine: Override audit logs.
Interview: Application programmer, if available, and user management personnel.

SI-10(FIS-6) – Enhancement (High)

Control

Transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.

Applicability: All	**References:** FISCAM: TCP-1.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-6).1

Assessment Objective

Determine if the organizational information system transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.

Assessment Methods And Objects

Examine: Application documentation.
Examine: Pertinent policies and procedures.
Examine: Supporting documentation generated by system.
Interview: Application programmer, if available.
Interview: User management and personnel.

SI-10(FIS-7) – Enhancement (High)

Control

Transactions are sequence checked and computer matched with data in master or suspense files to identify missing or duplicate transactions. Reports of missing or duplicate transactions are produced, and items are investigated and resolved in a timely manor.

Applicability: All	**References:** FISCAM: TCP-1.2.3, TCP-1.2.4, TCP-1.3.1, TCP-1.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-7).1

Assessment Objective

Determine if the organizational information system transactions are sequence checked and computer matched with data in master or suspense files to identify missing or duplicate transactions. Reports of missing or duplicate transactions are produced, and items are investigated and resolved in a timely manor.

Assessment Methods And Objects

Examine: Activity to investigate items reported as missing or duplicate.
Examine: Application documentation.
Examine: Pertinent policies and procedures.
Examine: Reports of missing and duplicate transactions.
Interview: Application programmer, if available.
Interview: User management and personnel.

SI-10(FIS-8) – Enhancement (High)

Control

Individual transactions or source documents are compared with a detailed listing of items processed by the computer, particularly to control important low-volume, high-value transactions.

Applicability: All; Optional for CWF	**References:** FISCAM: TCP-1.4.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-8).1

Assessment Objective

Determine if the organizational information system's individual transactions or source documents are compared with a detailed listing of items processed by the computer, particularly to control important low-volume, high-value transactions.

Assessment Methods And Objects

Examine: Comparison activity.
Examine: Listings for notations showing checking was performed.
Examine: Pertinent policies and procedures.
Interview: User management and personnel.

SI-11 – Error Handling (High)

Control

Information systems shall identify and handle error conditions in an expeditious manner. User error messages generated by information systems shall provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages shall be revealed only to authorized personnel. Sensitive information shall not be listed in error logs or associated administrative messages.

Guidance

The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Applicability: All	**References:** ARS: SI-11; FISCAM: TAY-3.2.1; NIST 800-53/53A: SI-11; PISP: 4.17.11	**Related Controls:** SI-2

ASSESSMENT PROCEDURE: SI-11.1

Assessment Objective

Determine if:
(i) the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries;
(ii) the information system reveals only essential information to authorized individuals; and
(iii) the information system does not include sensitive information in error logs or associated administrative messages.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system error handling capability.

SI-11(0) – Enhancement (High)

Control

Employ automated mechanisms that generate error messages providing timely and useful information to users without revealing information that could be exploited by adversaries. Ensure confidential information (e.g., account numbers, User IDs, social security numbers, etc.) is not listed in error logs or associated with administrative messages.

Applicability: All	**References:** ARS: SI-11(0); FISCAM: TAY-4.1.8; NIST 800-53/53A: SI-11; PISP: 4.17.11	**Related Controls:**

ASSESSMENT PROCEDURE: SI-11(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system error handling capability.

SI-11(FIS-1) – Enhancement (High)		
Control Rejected data are automatically written on an automated error suspense file and purged as corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error, (2) date and time the transaction was processed and the error identified, and (3) the identity of the user who originated the transaction. Record counts and control totals are established over the suspense file and used in reconciling transactions processed.		
Applicability: All	**References:** FISCAM: TAY-3.1.1, TAY-3.1.2, TAY-3.1.4	**Related Controls:**
ASSESSMENT PROCEDURE: SI-11(FIS-1).1		
Assessment Objective Determine if the organizational information system's rejected data is automatically written on an automated error suspense file and purged as corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error, (2) date and time the transaction was processed and the error identified, and (3) the identity of the user who originated the transaction. Record counts and control totals are established over the suspense file and used in reconciling transactions processed. **Assessment Methods And Objects** **Examine:** Application documentation and interview application programmers, if available. **Examine:** Reports produced from the suspense file. **Interview:** User management and personnel. **Test:** Verify process with test transactions containing errors.		
SI-11(FIS-2) – Enhancement (High)		
Control A control group is responsible for: reviewing suspense file control total reports, determining completeness of processing, and controlling and monitoring rejected transactions		
Applicability: All; Optional for CWF, SS	**References:** FISCAM: TAY-3.1.3	**Related Controls:**
ASSESSMENT PROCEDURE: SI-11(FIS-2).1		
Assessment Objective Determine if the organizational information system's control group is responsible for: reviewing suspense file control total reports, determining completeness of processing, and controlling and monitoring rejected transactions **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Reports produced from the suspense file. **Interview:** User management and control group. **Test:** Verify review process with test transactions containing errors.		
SI-11(FIS-3) – Enhancement (High)		
Control The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected transactions.		
Applicability: All; Optional for CWF, DC, EDC, SS	**References:** FISCAM: TAY-3.1.5	**Related Controls:**
ASSESSMENT PROCEDURE: SI-11(FIS-3).1		
Assessment Objective Determine if: (i) the organizational information system [The suspense file] is produced, on a regular basis for management review; and (ii) the organization determines the level and type of transaction errors and the age of uncorrected transactions. **Assessment Methods And Objects** **Examine:** Analysis reports produced from the suspense file. **Examine:** Application documentation. **Examine:** Pertinent policies and procedures. **Interview:** User management and control group.		
SI-11(FIS-4) – Enhancement (High)		
Control Errors are corrected by the user originating the transaction, and all corrections are reviewed and approved by supervisors before the corrections are reentered.		

Applicability: All	References: FISCAM: TAY-3.2.2, TAY-3.2.3	Related Controls:

ASSESSMENT PROCEDURE: SI-11(FIS-4).1

Assessment Objective

Determine if the organizational information system errors are corrected by the user originating the transaction, and all corrections are reviewed and approved by supervisors before the corrections are reentered.

Assessment Methods And Objects

Examine: Error correction activities.
Examine: Error reports.
Examine: Pertinent policies and procedures.
Interview: User management and personnel.
Test: Verify test transactions containing errors.

SI-11(FIS-5) – Enhancement (High)

Control

A control group is responsible for: reviewing control total reports, determining completeness of processing, and controlling and monitoring rejected transactions

Applicability: All; Optional for SS	References: FISCAM: TCP-2.1.5	Related Controls:

ASSESSMENT PROCEDURE: SI-11(FIS-5).1

Assessment Objective

Determine if the organizational control group is responsible for: reviewing control total reports, determining completeness of processing, and controlling and monitoring rejected transactions

Assessment Methods And Objects

Examine: Application documentation.
Examine: Pertinent policies and procedures.
Examine: Review and completeness of processing activities.
Interview: Data control personnel.
Interview: User management and personnel.

SI-12 – Information Output Handling and Retention (High)

Control

Output from information systems shall be handled and retained in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, operational requirements, and the information sensitivity level.

Guidance

A good place to obtain procedures for handling sensitive output information is the NIST SP.

Applicability: All	References: ARS: SI-12; FISCAM: TAY-4.1.6; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2; NIST 800-53/53A: SI-12; PISP: 4.17.12	Related Controls:

ASSESSMENT PROCEDURE: SI-12.1

Assessment Objective

Determine if:
(i) the organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and
(ii) the organization handles output from the information system in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records.
Interview: Organizational personnel with information output handling and retention responsibilities.

SI-12(CMS-1) – Enhancement (High)

Control

Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements.

Applicability: All	References: ARS: SI-12(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2	Related Controls:

ASSESSMENT PROCEDURE: SI-12(CMS-1).1

Assessment Objective

Determine if the organization retains output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable NARA requirements.

Assessment Methods And Objects

Examine: At a minimum, documentation for record retention of audit records, system reports, business and financial reports, and business records are in accordance with CMS Policy and all applicable NARA requirements.

SI-12(FIS-1) – Enhancement (High)

Control

Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design by a data processing control group, or some alternative. A data processing control group: (1) has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; (2) reviews output products for general acceptability; and (3) reconciles control information to determine completeness of processing.

Applicability: All	References: FISCAM: TAY-4.1.1, TAY-4.1.2	Related Controls:

ASSESSMENT PROCEDURE: SI-12(FIS-1).1

Assessment Objective

Determine if the organization assigns responsibility for seeing that all outputs are produced and distributed according to system requirements and design by a data processing control group, or some alternative. A data processing control group: (1) has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; (2) reviews output products for general acceptability; and (3) reconciles control information to determine completeness of processing.

Assessment Methods And Objects

Examine: Output production and distribution.

Examine: Pertinent policies and procedures.

Interview: Information system and user management.

SI-12(FIS-2) – Enhancement (High)

Control

Printed reports contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message.

Applicability: All	References: FISCAM: TAY-4.1.3	Related Controls:

ASSESSMENT PROCEDURE: SI-12(FIS-2).1

Assessment Objective

Determine if the organizational information system printed reports contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message.

Assessment Methods And Objects

Examine: Application documentation.

Examine: Printed reports.

Interview: User personnel and application programmer, if available.

SI-12(FIS-3) – Enhancement (High)

Control

Each output produced, whether printed or transmitted to a user's terminal device, is logged, manually if not automatically, including the recipient(s) who receive the output.

Applicability: All	References: FISCAM: TAY-4.1.4, TAY-4.1.5	Related Controls:

ASSESSMENT PROCEDURE: SI-12(FIS-3).1

Assessment Objective

Determine if the organizational information system's output produced, whether printed or transmitted to a user's terminal device, is logged, manually if not automatically, including the recipient(s) who receive the output.

Assessment Methods And Objects

Examine: Application documentation.

Examine: Output logs.

Interview: Information system and user personnel.

SI-12(FIS-4) – Enhancement (High)		
Control In the user department, outputs transmitted are summarized daily and printed for each terminal device, and reviewed by supervisors. A control log of output product errors is maintained, including the corrective actions take.		
Applicability: All	**References:** FISCAM: TAY-4.1.7, TAY-4.1.8	**Related Controls:**
ASSESSMENT PROCEDURE: SI-12(FIS-4).1		
Assessment Objective Determine if the organizational information system's user department, outputs transmitted are summarized daily and printed for each terminal device, and reviewed by supervisors. A control log of output product errors is maintained, including the corrective actions take. **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Supporting documentation (e.g., printed daily summaries with supervisory initials or signatures). **Examine:** This activity. **Interview:** User supervisory personal.		
SI-12(FIS-5) – Enhancement (High)		
Control Users review output reports for data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction reports, (3) master record change reports, (4) exception reports, and (5) control totals balance reports. Output from reruns is subjected to the same quality review as the original output.		
Applicability: All	**References:** FISCAM: TAY-4.1.9, TAY-4.2.1	**Related Controls:**
ASSESSMENT PROCEDURE: SI-12(FIS-5).1		
Assessment Objective Determine if the organizational users review output reports for data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction reports, (3) master record change reports, (4) exception reports, and (5) control totals balance reports. Output from reruns is subjected to the same quality review as the original output. **Assessment Methods And Objects** **Examine:** Activity to review output reports. **Examine:** Output reports. **Examine:** Pertinent policies and procedures. **Interview:** User management and personnel.		

Business Partners Systems Security Manual

Appendix A, Attachment 2

CMS Core Security Requirements (CSR)

for

Moderate Impact Level Assessments

CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

Rev. 9

(This page intentionally left blank)

Access Control (AC) – *Technical*

AC-1 – Access Control Policy and Procedures (Moderate)

Control

Logical access controls and procedures shall be established and implemented effectively to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (i.e., programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

Guidance

The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AC-1; FISCAM: TAC-3.2.C.1, TAC-4.3.4, TSD-1.1.1, TSD-2.1, TSS-1.1.1; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1; NIST 800-53/53A: AC-1; PISP: 4.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents access control policy and procedures;
(ii) the organization disseminates access control policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review access control policy and procedures; and
(iv) the organization updates access control policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.
Interview: Organizational personnel with access control responsibilities.(Optional)

ASSESSMENT PROCEDURE: AC-1.2

Assessment Objective

Determine if:
(i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.
Interview: Organizational personnel with access control responsibilities.(Optional)

AC-1(FIS-1) – Enhancement (Moderate)

Control

Standard forms are used to document approval for archiving, deleting, or sharing data files. Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

Applicability: All	**References:** FISCAM: TAC-2.3.1, TAC-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-1(FIS-1).1

Assessment Objective

Determine if:
(i) the organization uses standard forms to document approval for archiving, deleting, or sharing data files; and
(ii) the organizational agreements, with other entities, document prior to sharing data or programs how the data files are protected.

Assessment Methods And Objects

Examine: Documents authorizing file sharing and file sharing agreements.
Examine: Pertinent policies and procedures.
Examine: Standard approval forms.
Interview: Data owners.

AC-2 – Account Management (Moderate)

Control

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. Access to the CMS information system shall be granted based on: (a) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (b) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

Guidance

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

Applicability: All	**References:** ARS: AC-2; FISCAM: TAC-3.2.C.4, TAC-3.2.C.5, TSP-4.1.6, TSS-1.1.3; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2.1

Assessment Objective

Determine if:
(i) the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts;
(ii) the organization defines the frequency of information system account reviews;
(iii) the organization reviews information system accounts at the organization-defined frequency, at least annually; and
(iv) the organization initiates required actions on information system accounts based on the review.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing account management; information system security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.
Interview: Organizational personnel with account management responsibilities.

AC-2(0) – Enhancement (Moderate)

Control

Review information system accounts every 180 days and require annual certification.

Applicability: All	**References:** ARS: AC-2(0); FISCAM: TAC-3.2.C.4, TSS-1.1.4; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records.
Interview: Organizational personnel with account management responsibilities.

AC-2(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to support the management of information system accounts.

Applicability: All	**References:** ARS: AC-2(1); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to support information system account management functions.

Assessment Methods And Objects

Examine: Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.(Optional)

AC-2(2) – Enhancement (Moderate)

Control

Configure the information system to allow emergency account for a period of time NTE 24 hours and to allow accounts with a fixed duration (i.e., temporary accounts) NTE 365 days.

Applicability: All	**References:** ARS: AC-2(2); FISCAM: TAC-2.2; IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(2).1

Assessment Objective

Determine if:

(i) the organization defines a time period after which the information system terminates temporary and emergency accounts; and

(ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.

Assessment Methods And Objects

Examine: Information system security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.(Optional)

AC-2(3) – Enhancement (Moderate)

Control

Configure the information system to disable inactive accounts automatically after 180 days.

Applicability: All	**References:** ARS: AC-2(3); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(3)	**Related Controls:** IA-4(0)

ASSESSMENT PROCEDURE: AC-2(3).1

Assessment Objective

Determine if:

(i) the organization defines a time period after which the information system disables inactive accounts; and

(ii) the information system automatically disables inactive accounts after organization-defined time period.

Assessment Methods And Objects

Examine: Procedures addressing account management; information system security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.(Optional)

AC-2(4) – Enhancement (Moderate)

Control

Employ automated mechanisms to audit user account creation, modification, disabling, and termination. Ensure the automated mechanism notifies appropriate personnel of the user account management actions.

Applicability: All	**References:** ARS: AC-2(4); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(4)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(4).1

Assessment Objective

Determine if:

(i) the organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions; and

(ii) the organization employs automated mechanisms to notify, as required, appropriate individuals.

Assessment Methods And Objects

Examine: Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.(Optional)

AC-2(CMS-1) – Enhancement (Moderate)		
Control Remove or disable default user accounts. Rename active default accounts.		
Applicability: All	**References:** ARS: AC-2(CMS-1); FISCAM: TAC-3.2.A.3, TAC-3.2.C.4, TSS-1.2.3; IRS-1075: 5.6.3.2#2.1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(CMS-1).1		
Assessment Objective Determine if the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. **Assessment Methods And Objects** **Examine:** Access control policy and procedures; other relevant documents or records to determine if the organization removes or disables default user accounts. It must also rename active default accounts if they must be used. **Interview:** Organizational personnel with access control responsibilities to determine that all default user accounts are either removed or disabled. If default accounts are active, that they are renamed. **Test:** Information system sample of hosts with defined users to ensure that all default user accounts are either removed or disabled. If default accounts are active, that they are renamed.		
AC-2(CMS-2) – Enhancement (Moderate)		
Control Require the use of unique and separate administrator accounts for administrator and non-administrator activities.		
Applicability: All	**References:** ARS: AC-2(CMS-2); FISCAM: TAN-2.1.4; IRS-1075: 5.6.3.2#2.1	**Related Controls:** IA-4(CMS-1)
ASSESSMENT PROCEDURE: AC-2(CMS-2).1		
Assessment Objective Determine if the information system enforces separation of duties through assigned access authorizations. **Assessment Methods And Objects** **Examine:** Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if the organization prohibits administrator accounts to be used for day-to-day activities. **Interview:** Organizational personnel with account management responsibilities to determine if administrator accounts are being used for day to day activities. **Test:** Information system sample of hosts' system logs to ensure that administrator accounts are not being used for day-to-day activities.		
AC-2(CMS-3) – Enhancement (Moderate)		
Control Implement centralized control of user access administrator functions.		
Applicability: All	**References:** ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(CMS-3).1		
Assessment Objective Determine if the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. **Assessment Methods And Objects** **Examine:** Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if all user access administrator functions are centralized. **Interview:** Organizational personnel with account management responsibilities to determine if all user access administrator functions are carried out by a centralized administrator function. **Test:** Information system sample of hosts' system logs to determine if all user access administrator functions are carried out by a centralized administrator function.		
AC-2(CMS-4) – Enhancement (Moderate)		
Control Regulate the access provided to contractors and define security requirements for contractors.		
Applicability: All	**References:** ARS: AC-2(CMS-4); IRS-1075: 5.6.3.2#2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(CMS-4).1

Assessment Objective

Determine if the organization documents contractor security requirements and maintains contractor access privileges.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if all contractors' access are authorized, regulated, and security requirements for contractors are defined.

Interview: Organizational personnel with account management responsibilities to determine if written authorizations exist for a sample of contractor employees.

AC-2(CMS-5) – Enhancement (Moderate)

Control

Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked prior to or during the termination process.

Applicability: All	**References:** ARS: AC-2(CMS-5); FISCAM: TSP-4.1.6; IRS-1075: 5.6.3.2#2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(CMS-5).1

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine when employee access rights are revoked on termination.

Interview: Organizational personnel with personnel security responsibilities to determine when access is revoked on employee termination.

AC-2(FIS-1) – Enhancement (Moderate)

Control

All system access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to security managers.

Guidance

The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties.

Applicability: All	**References:** FISCAM: TAC-2.1.1, TAC-2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(FIS-1).1

Assessment Objective

Determine if:

(i) the organization grants system access authorizations on standard forms and maintains the completed forms on file; and

(ii) the organizational senior managers approve system access authorizations and the approvals are securely transferred to security managers.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Selection of user (both application user and information system personnel) access authorization documentation.

Interview: Personnel involved in access authorizations and senior managers who approve authorizations.

AC-2(FIS-2) – Enhancement (Moderate)

Control

Business Owners periodically review system access authorization listings and determine whether they remain appropriate. ISSO/SSOs review system access authorizations and discuss any questionable authorizations with Business Owners.

Applicability: All	**References:** FISCAM: TAC-2.1.2, TAC-2.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(FIS-2).1

Assessment Objective

Determine if the organization ISSO/SSOs periodically reviews system access authorization listings and discusses questionable authorizations with management.

Assessment Methods And Objects

Examine: Access authorization listings to determine whether inappropriate access are removed in a timely manner.

Examine: Pertinent policies and procedures.
Interview: Business Owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner.
Interview: ISSO/SSOs and review documentation provided to them.

AC-3 – Access Enforcement (Moderate)

Control

Access enforcement mechanisms shall be developed, documented and implemented effectively to control access between named users (or processes) and named objects (e.g., files and programs) in a CMS information system. Additional application level access enforcement mechanism shall be implemented, when necessary, to provide increased information security for CMS information. When encryption of stored information is employed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (see section 4.16.13).

Guidance

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

Applicability: All	**References:** ARS: AC-3; FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.C.6, TAC-3.2.D.1, TCC-3.2.3, TSS-2.1.1, TSS-2.1.2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3; NIST 800-53/53A: AC-3; PISP: 4.1.3	**Related Controls:** MA-CMS-1, MA-CMS-2, SC-13

ASSESSMENT PROCEDURE: AC-3.1

Assessment Objective

Determine if:
(i) the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy; and
(ii) user privileges on the information system are consistent with the documented user authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing access enforcement policy.(Optional)

AC-3(1) – Enhancement (Moderate)

Control

Ensure the information system restricts access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.

Guidance

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Applicability: All	**References:** ARS: AC-3(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.2, TAC-3.2.C.5, TAC-3.2.D.1, TCC-3.2.3, TSD-3.1.4, TSS-1.1.2, TSS-2.1.2; IRS-1075: 5.6.3.2#2.2; NIST 800-53/53A: AC-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-3(1).1

Assessment Objective

Determine if:
(i) the organization explicitly defines privileged functions and security-relevant information for the information system;
(ii) the organization explicitly authorizes personnel access to privileged functions and security-relevant information in accordance with organizational policy; and
(iii) the information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel (e.g., security administrators).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing access enforcement policy.(Optional)

AC-3(CMS-1) – Enhancement (Moderate)		
Control If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).		
Applicability: All	**References:** ARS: AC-3(CMS-1); IRS-1075: 5.6.3.2#2.2	**Related Controls:** SC-13
ASSESSMENT PROCEDURE: AC-3(CMS-1).1		
Assessment Objective Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. **Assessment Methods And Objects** **Examine:** Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if encryption is used as an access control mechanism, examine system and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13). **Interview:** Organizational personnel with access control responsibilities to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13). **Test:** Information system if encryption is used as an access control mechanism; examine organization's encryption key lengths, algorithms, certificates, etc.		
AC-3(CMS-2) – Enhancement (Moderate)		
Control If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix A for e-Authentication Standards.		
Applicability: All	**References:** ARS: AC-3(CMS-2); IRS-1075: 5.6.3.2#2.2	**Related Controls:**
ASSESSMENT PROCEDURE: AC-3(CMS-2).1		
Assessment Objective Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users). **Assessment Methods And Objects** **Examine:** Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if e-authentication is used as an access control mechanism, examine Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the organization's encryption standard meets ARS Appendix A for e-Authentication Standards. **Interview:** Organizational personnel with access control responsibilities if e-authentication is used as an access control mechanism, interview system administrators responsible for the hosts providing authentication services to determine if the organization meets the standards described in ARS Appendix A. **Test:** Information system if e-authentication is used as an access control mechanism; test a sample of hosts for automated mechanisms implementing identification and authentication capability for the information system.		
AC-3(CMS-3) – Enhancement (Moderate)		
Control Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information.		
Applicability: All	**References:** ARS: AC-3(CMS-3); FISCAM: TAC-3.2.D.1, TCC-3.2.3; IRS-1075: 5.6.2.3#1, 5.6.3.2#2.2	**Related Controls:**
ASSESSMENT PROCEDURE: AC-3(CMS-3).1		
Assessment Objective Determine if the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements. **Assessment Methods And Objects** **Examine:** Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive		

information.

Interview: Organizational personnel with access control responsibilities to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

Test: Automated mechanisms implementing access enforcement policy to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

AC-3(CMS-4) – Enhancement (Moderate)

Control

Data stored in the information system must be protected with system access controls.

Applicability: All	References: ARS: AC-3(CMS-4); FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.D.1, TAY-3.1.6, TCC-3.2.3; HIPAA: 164.312(a)(2)(iv); IRS-1075: 5.6.3.2#2.2	Related Controls:

ASSESSMENT PROCEDURE: AC-3(CMS-4).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if data stored in the information system is protected with system access controls and must be encrypted when residing in non-secure areas.

Interview: Organizational personnel with access control responsibilities to determine if hosts storing data are protected with system access controls and if data stored in non-secure areas are encrypted.

Test: Automated mechanisms implementing access enforcement policy to if data stored on these hosts is protected with system access controls and that it is encrypted if residing in non-secure areas.

AC-4 – Information Flow Enforcement (Moderate)

Control

Flow control shall be enforced over information between source and destination objects within CMS information systems and between interconnected systems based on the characteristics of the information.

Guidance

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

Applicability: All	References: ARS: AC-4; IRS-1075: 5.6.3.2#2.2; NIST 800-53/53A: AC-4; PISP: 4.1.4	Related Controls: SC-7

ASSESSMENT PROCEDURE: AC-4.1

Assessment Objective

Determine if the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information flow enforcement policy.(Optional)

ASSESSMENT PROCEDURE: AC-4.2

Assessment Objective

Determine if interconnection agreements address the types of permissible and impermissible flow of information between information systems and the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system interconnection agreements; information system configuration settings and associated

documentation; list of information flow control authorizations; information system audit records; other relevant documents or records.

AC-5 – Separation of Duties (Moderate)

Control

The principle of separation of duties shall be enforced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission functions and distinct information systems support functions shall be divided among different roles, and support functions shall be performed by different individuals (e.g., personnel responsible for administering access control functions shall not also administer audit functions). Personnel developing and testing system code shall not have access to production libraries. Access control software shall be in place to limit individual authority and information access, such that the collusion of two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties.

Guidance

The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Applicability: All	References: ARS: AC-5; FISCAM: TAY-1.3.2, TSD-1.1.1, TSD-1.1.2, TSD-1.1.3, TSD-1.1.5, TSD-1.2.1, TSD-1.3.3, TSD-2.2.2, TSS-1.1.2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3; NIST 800-53/53A: AC-5; PISP: 4.1.5	Related Controls:

ASSESSMENT PROCEDURE: AC-5.1

Assessment Objective

Determine if:
(i) the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and
(ii) the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing separation of duties; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records.
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties.(Optional)
Test: Automated mechanisms implementing separation of duties policy.(Optional)

AC-5(CMS-1) – Enhancement (Moderate)

Control

Ensure that audit functions are not performed by security personnel responsible for administering access control.

Applicability: All	References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5	Related Controls:

ASSESSMENT PROCEDURE: AC-5(CMS-1).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if audit functions are NOT performed by security personnel responsible for administering access control. Also, ensure that the organization enforces separation of duties through assigned access authorizations.
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are NOT performed by security personnel. Also, determine if access authorizations complement and reinforce separation of duties.
Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-2) – Enhancement (Moderate)

Control

Maintain a limited group of administrators with access based upon the users' roles and responsibilities.

Applicability: All	References: ARS: AC-5(CMS-2)	Related Controls:

ASSESSMENT PROCEDURE: AC-5(CMS-2).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization maintains a limited group of administrators with access based upon the users' roles and responsibilities.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the number of personnel with root access is limited to only those personnel with a business need for root access.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-3) – Enhancement (Moderate)

Control

Ensure that critical mission functions and information system support functions are divided among separate individuals.

Applicability: All	**References:** ARS: AC-5(CMS-3); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-3).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-4) – Enhancement (Moderate)

Control

Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Applicability: All	**References:** ARS: AC-5(CMS-4); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-4).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-5) – Enhancement (Moderate)

Control

Ensure that an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.

Applicability: All	**References:** ARS: AC-5(CMS-5); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-5).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the

information system, conducts information security testing of the information system.
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties. None of these individuals or functions should be conducting information security testing of the information system.
Test: Automated mechanisms implementing separation of duties policy.

AC-5(FIS-1) – Enhancement (Moderate)

Control

Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.

Applicability: All	**References:** FISCAM: TSD-1.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(FIS-1).1

Assessment Objective

Determine if the organization provides adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Interview: Personnel to determine whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.

AC-6 – Least Privilege (Moderate)

Control

Each user or process shall be assigned the most restrictive set of privileges needed for the performance of authorized tasks.

Guidance

The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Applicability: All	**References:** ARS: AC-6; FISCAM: TSD-2.1; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); HSPD 7: D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2; NIST 800-53/53A: AC-6; PISP: 4.1.6	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6.1

Assessment Objective

Determine if:
(i) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks; and
(ii) the information system enforces the most restrictive set of rights/privileges or accesses needed by users.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.(Optional)

AC-6(CMS-1) – Enhancement (Moderate)

Control

Disable all file system access not explicitly required for system, application, and administrator functionality.

Applicability: All	**References:** ARS: AC-6(CMS-1); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6(CMS-1).1

Assessment Objective

Determine if the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if all file system access not explicitly required for system, application, and administrator functionality is disabled.
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine hosts that store, transmit or process sensitive data to determine if file system access not explicitly required for system, application, and administrator functionality are disabled.
Test: Information system hosts that store, transmit or process sensitive data to ensure that all file system access not explicitly required for system, application, and administrator functionality is

disabled.

AC-6(CMS-2) – Enhancement (Moderate)

Control

Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.

Applicability: All	**References:** ARS: AC-6(CMS-2); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6(CMS-2).1

Assessment Objective

Determine if the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if contractors are required to be provided with minimal system and physical access, and that they've agreed to support the CMS security requirements. The documented contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine the default access levels given to contractors. Ensure that all file system access not explicitly required for system, application, and administrator functionality is disabled.

Test: Information system hosts that store, transmit or process sensitive data; and that contain account information for contractors, to determine if all file system access not explicitly required for system, application, and administrator functionality is disabled.

AC-6(CMS-3) – Enhancement (Moderate)

Control

Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.

Applicability: All	**References:** ARS: AC-6(CMS-3); FISCAM: TAC-3.2.D.1, TAC-3.2.D.2, TAC-3.2.D.3, TAC-3.2.D.4	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6(CMS-3).1

Assessment Objective

Determine if the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system restricts the use of database management utilities to only authorized database administrators. Policies and procedures must also prevent users from accessing database data files at the logical data view, field, or field-value levels. Implement column-level access controls.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine if the information system restricts the use of database management utilities to only authorized database administrators. Also, determine whether or not users are prevented from accessing database data files at the logical data view, field, or field-value levels. Column-level access controls must also be implemented.

Test: Information system hosting databases to determine if the information system restricts the use of database management utilities to only authorized database administrators. Also, determine whether or not users are prevented from accessing database data files at the logical data view, field, or field-value levels. Column-level access controls must also be implemented.

AC-6(CMS-4) – Enhancement (Moderate)

Control

Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.

Applicability: All	**References:** ARS: AC-6(CMS-4); FISCAM: TAN-2.2.1; HIPAA: 164.312(c)(1); HSPD 7: D(10); IRS-1075: 5.1#1.1, 5.2#1, 5.2#2, 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6(CMS-4).1

Assessment Objective

Determine if the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine if the default level of access for the various user types. Ensure that only access to those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties are assigned.
Test: Information system using a sample of user accounts with limited access, attempt to access files, directories, drives, workstations, servers, network shares, ports, protocols, or services that this user or user type has no access to.

AC-7 – Unsuccessful Log-on Attempts (Moderate)

Control

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce a limit of CMS-defined consecutive invalid access attempts by a user during a specified time period. Systems shall be locked after a specified number of multiple unsuccessful log-on attempts.

Guidance

Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Applicability: All	**References:** ARS: AC-7; IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7	**Related Controls:**

ASSESSMENT PROCEDURE: AC-7.1

Assessment Objective

Determine if:
(i) the organization defines the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur;
(ii) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period;
(iii) the organization defines the time period for lock out mode or delay period;
(iv) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; and
(v) the information system enforces the organization-selected lock out mode or delayed login prompt.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing unsuccessful logon attempts; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts.(Optional)

AC-7(0) – Enhancement (Moderate)

Control

Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user during a fifteen (15) minute time period. Require the lock out to persist for a minimum of one (1) hour.

Applicability: All	**References:** ARS: AC-7(0); IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7	**Related Controls:** AC-9

ASSESSMENT PROCEDURE: AC-7(0).1

Assessment Objective

Determine if the organization configures system lockout to assist in preventing password guessing.

Assessment Methods And Objects

Examine: Password lockout policy includes failed log-on attempts, lockout timeframes period for failed attempts and system/network administrator account reset capabilities.
Interview: A sampling of users for knowledge of log-on and account lockout procedure policy is known.
Test: The account lockout function requires and administrator's reset of the locked-out user account.

AC-8 – System Use Notification (Moderate)

Control

An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS information system.

Guidance

Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is

displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Applicability: All	**References:** ARS: AC-8; FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2; NIST 800-53/53A: AC-8; PISP: 4.1.8	**Related Controls:** SI-4

ASSESSMENT PROCEDURE: AC-8.1

Assessment Objective

Determine if:
(i) the information system displays a system use notification message before granting system access informing potential users:
- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording;
(ii) the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).
(iii) the organization approves the information system use notification message before its use; and
(iv) the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for system use notification.(Optional)

AC-8(CMS-1) – Enhancement (Moderate)

Control

Configure the information system to display a warning banner automatically prior to granting access to potential users. Notify users that:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.

Guidance

All CMS information system computers and network devices under their control, independently, prominently and completely display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web, ftp, telnet, or other services accessed.

Applicability: All	**References:** ARS: AC-8(CMS-1); FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-1).1

Assessment Objective

Determine if the information system displays a system use notification message before granting system access informing potential users:
- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if the information system is configured to display a warning banner automatically prior to granting access to potential users. Notify users that:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.
Interview: Organizational personnel to determine if hosts are configured to present a warning banner at system access points. The warning banner must contain the following elements:
(a) They are accessing a U.S. Government information system;

(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.
Test: Automated mechanisms implementing the access control policy for system use notification.

AC-8(CMS-2) – Enhancement (Moderate)

Control

Develop and implement the warning banner in conjunction with legal counsel.

Applicability: All	**References:** ARS: AC-8(CMS-2); IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-2).1

Assessment Objective

Determine if the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if warning banners were developed and implemented in conjunction with legal counsel.
Interview: Organizational personnel to determine if warning banners were developed and implemented in conjunction with legal counsel.
Test: Automated mechanisms implementing the access control policy for system use notification.(Optional)

AC-8(CMS-3) – Enhancement (Moderate)

Control

Post clear privacy policies on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.

Applicability: All	**References:** ARS: AC-8(CMS-3); IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-3).1

Assessment Objective

Determine if the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if clear privacy policies are posted on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.
Interview: Organizational personnel to determine if clear privacy policies are posted where substantial personal information from the public is collected.
Test: Automated mechanisms implementing the access control policy for system use notification.

AC-10 – Concurrent Session Control (Moderate)

Control

Automated mechanisms shall be in place to limit the number of concurrent user sessions, based upon the established business needs of the user, CMS, and the sensitivity level of the CMS information system.

Guidance

Some systems may require concurrent user sessions to function properly. However, based on the operational needs, automated mechanisms limit the number of concurrent user sessions. It is good practice to have management's approval for any system to have user concurrent sessions. Management should periodically review the need for user concurrent sessions.

Applicability: All	**References:** ARS: AC-10; NIST 800-53/53A: AC-10; PISP: 4.1.10	**Related Controls:**

ASSESSMENT PROCEDURE: AC-10.1

Assessment Objective

Determine if:
(i) the organization defines the maximum number of concurrent sessions for information system users; and
(ii) the information system limits the number of concurrent sessions for users to the organization-defined number of sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing the access control policy for concurrent session control.(Optional)

AC-10(0) – Enhancement (Moderate)

Control

The number of concurrent User ID network log-on sessions is limited and enforced to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties.

Applicability: All	**References:** ARS: AC-10(0), 4.1.10	**Related Controls:**

ASSESSMENT PROCEDURE: AC-10(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan (for organization-defined limit for concurrent sessions for information system users); other relevant documents or records.

AC-10(CMS-1) – Enhancement (Moderate)

Control

The requirement and use of more than one (1) application/process session for each user is documented in the SSP.

Applicability: All	**References:** ARS: AC-10(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-10(CMS-1).1

Assessment Objective

Determine if the information system limits the number of concurrent sessions for users to the organization-defined number of sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan (for organization-defined limit for concurrent sessions for information system users); other relevant documents or records to determine if the requirement and use of more than one (1) User ID network log-on session for each user is documented in the system risk assessment.

Interview: Organizational personnel to determine if the information system allows more than one log-on session.

Test: Automated mechanisms implementing the access control policy for concurrent session control.

AC-11 – Session Lock (Moderate)

Control

Automated session lock mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable locking of the information system session by the user. The information system shall also detect inactivity and block further access until the user re-establishes the connection using proper identification and authentication processes.

Guidance

Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.

Applicability: All	**References:** ARS: AC-11; IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-11; PISP: 4.1.11	**Related Controls:**

ASSESSMENT PROCEDURE: AC-11.1

Assessment Objective

Determine if:
(i) the organization defines the time period of user inactivity that initiates a session lock within the information system;
(ii) the information system initiates a session lock after the organization-defined time period of inactivity; and
(iii) the information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for session lock.(Optional)

AC-11(0) – Enhancement (Moderate)

Control

Configure systems to disable local access automatically after fifteen (15) minutes of inactivity. Require a password (see IA-5, Authenticator Management) to restore local access.

Applicability: All	**References:** ARS: AC-11(0); FISCAM: TAC-3.2.C.3; IRS-1075: 5.6.3.2#4.3, 5.7.3#1; NIST 800-53/53A: AC-11; PISP: 4.1.11	**Related Controls:** IA-5

ASSESSMENT PROCEDURE: AC-11(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; information system security plan (for organization-defined time period for user inactivity after which automatic session lock is to be activated); other relevant documents or records.

AC-12 – Session Termination (Moderate)

Control

The information system shall identify and terminate all inactive remote sessions (both user and information system sessions) automatically.

Guidance

A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Applicability: All	**References:** ARS: AC-12; FISCAM: TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-12; PISP: 4.1.12	**Related Controls:**

ASSESSMENT PROCEDURE: AC-12.1

Assessment Objective

Determine if:
(i) the organization defines the time period of user inactivity that initiates a remote session termination within the information system; and
(ii) the information system automatically terminates a remote session after the organization-defined time period of inactivity.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for session termination.(Optional)

AC-12(0) – Enhancement (Moderate)

Control

Configure the information system to automatically terminate all remote sessions (user and information system) after 30 minutes of inactivity.

Applicability: All	**References:** ARS: AC-12(0); FISCAM: TAC-3.2.C.3, TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-12; PISP: 4.1.12	**Related Controls:**

ASSESSMENT PROCEDURE: AC-12(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; information system security plan (for organization-defined time period for user inactivity after which automatic session termination is to be activated); other relevant documents or records.

AC-13 – Supervision and Review—Access Control (Moderate)

Control

Personnel shall be supervised and reviewed with respect to the usage of CMS information system access controls. Automated mechanisms shall be in place to facilitate the review of audit records, and any unusual activities shall be investigated in a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of users with significant information system roles and responsibilities shall be reviewed more frequently.

Guidance

The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	References: ARS: AC-13; FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSD-3.2.1, TSD-3.2.3, TSS-2.1.3; HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: AC-13; PISP: 4.1.13	Related Controls:

ASSESSMENT PROCEDURE: AC-13.1

Assessment Objective

Determine if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records.

Interview: Organizational personnel with supervisory and access control responsibilities.(Optional)

AC-13(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to facilitate the review of user activities.

Applicability: All	References: ARS: AC-13(1); NIST 800-53/53A: AC-13(1)	Related Controls:

ASSESSMENT PROCEDURE: AC-13(1).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.(Optional)

AC-13(CMS-1) – Enhancement (Moderate)

Control

Review integrity of files and directories for unexpected and/or unauthorized changes at least once per day. Automate the review of file creation, changes and deletions; and monitor permission changes. Generate alert notification for technical staff review and assessment.

Applicability: All	References: ARS: AC-13(CMS-1); FISCAM: TAC-2.1.5; HIPAA: 164.312(c)(2), 164.312(e)(2)(i)	Related Controls:

ASSESSMENT PROCEDURE: AC-13(CMS-1).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records to determine if files and directories are reviewed for unexpected and/or unauthorized changes at least once per day. The review of file creation, changes and deletions, and permission changes must be monitored automatically. Alert notifications must be generated for technical staff review and assessment.

Interview: Organizational personnel with supervisory and access control responsibilities to determine if the integrity of files and directories for unexpected and/or unauthorized changes at least once per day. Determine if file creation, changes and deletions, and permission changes are being reviewed automatically. Determine if alert notifications for technical staff review and assessment are being generated.

Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.

AC-13(CMS-2) – Enhancement (Moderate)

Control

Enable logging of administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations.

Applicability: All	References: ARS: AC-13(CMS-2); FISCAM: TAC-2.1.5, TAN-2.1.8, TSS-2.1.3	Related Controls:

ASSESSMENT PROCEDURE: AC-13(CMS-2).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records to determine if logging of administrator and user account activities, system shutdowns, reboots, errors and access

authorizations is enabled.
Interview: Organizational personnel with supervisory and access control responsibilities to determine if logging of administrator and user account activities, system shutdowns, reboots, errors and access authorizations is enabled.
Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.

AC-13(CMS-3) – Enhancement (Moderate)

Control

Inspect administrator groups, root accounts and other system related accounts on demand but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.

Applicability: All	**References:** ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(CMS-3).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system related accounts are inspected on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.
Interview: Organizational personnel with supervisory and access control responsibilities to determine if administrator groups, root accounts and other system related accounts are inspected on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.
Test: Automated mechanisms supporting the access control policy for supervision and review of user.

AC-13(FIS-1) – Enhancement (Moderate)

Control

Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

Applicability: All	**References:** FISCAM: TSD-1.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(FIS-1).1

Assessment Objective

Determine if the organizational supervisory personnel review transactions performed.

Assessment Methods And Objects

Examine: Activities and test transaction reviews.
Examine: Pertinent policies and procedures.
Interview: Management.

AC-14 – Permitted Actions without Identification or Authentication (Moderate)

Control

Based upon mission / business requirements, public access to CMS information systems without identification and authorization shall be limited to public websites and other publicly available systems. CMS information systems shall be configured to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

Guidance

The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov).

Applicability: All	**References:** ARS: AC-14; NIST 800-53/53A: AC-14; PISP: 4.1.14	**Related Controls:** IA-2

ASSESSMENT PROCEDURE: AC-14.1

Assessment Objective

Determine if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for permitted actions without identification and authentication.(Optional)

AC-14(0) – Enhancement (Moderate)		
Control Identify and document specific user actions that can be performed on the information system without identification or authentication.		
Applicability: All	**References:** ARS: AC-14(0); NIST 800-53/53A: AC-14; PISP: 4.1.14	**Related Controls:**
ASSESSMENT PROCEDURE: AC-14(0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.		
AC-14(1) – Enhancement (Moderate)		
Control Ensure that public users (users who have not been authenticated) only have access to the extent necessary to accomplish mission objectives while preventing unauthorized access to sensitive information.		
Applicability: All	**References:** ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1)	**Related Controls:**
ASSESSMENT PROCEDURE: AC-14(1).1		
Assessment Objective Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; list of organization-defined actions that can be performed without identification and authentication; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for defining permitted actions without identification and authentication.(Optional)		
AC-16 – Automated Labeling (Moderate)		
Control CMS information systems shall label information “in storage,” “in process,” and “in transit” with special dissemination handling or distribution instructions, in a manner consistent with this policy.		
Guidance Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.		
Applicability: All	**References:** ARS: AC-16; NIST 800-53/53A: AC-16; PISP: 4.1.16	**Related Controls:** AC-15
ASSESSMENT PROCEDURE: AC-16.1		
Assessment Objective Determine if the information system appropriately labels information in storage, in process, and in transmission. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional) **Test:** Automated mechanisms implementing automated (internal) labeling within the information system.(Optional)		
AC-16(CMS-1) – Enhancement (Moderate)		
Control If automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).		
Applicability: All	**References:** ARS: AC-16(CMS-1)	**Related Controls:**
ASSESSMENT PROCEDURE: AC-16(CMS-1).1		
Assessment Objective Determine if the information system appropriately labels information in storage, in process, and in transmission. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system		

configuration settings and associated documentation; other relevant documents or records to determine, if automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

Interview: Organization personnel to determine, if automated information labeling is utilized, that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

Test: Automated mechanisms implementing automated (internal) labeling within the information system.

AC-17 – Remote Access (Moderate)

Control

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can access the information system from remote locations shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, shall not be used to gain access to a CMS information system that processes CMS sensitive information unless the CIO or his/her designated representative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-up capabilities.

Guidance

Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST SP 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 and 800-78. NIST SP 800-77 provides guidance on IPSec-based virtual private networks.

Applicability: All	**References:** ARS: AC-17; FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17; PISP: 4.1.17	**Related Controls:** IA-2, SC-9

ASSESSMENT PROCEDURE: AC-17.1

Assessment Objective

Determine if the organization documents, monitors, and controls all methods of remote access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities.

AC-17(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to facilitate the monitoring and control of remote access methods.

Applicability: All	**References:** ARS: AC-17(1); IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(1).1

Assessment Objective

Determine if the information system employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for remote access.(Optional)

AC-17(2) – Enhancement (Moderate)

Control

Employ cryptography to protect the confidentiality and integrity of remote access sessions.

Applicability: All	**References:** ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(2).1

Assessment Objective

Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing cryptographic protections for remote access.(Optional)

AC-17(3) – Enhancement (Moderate)

Control

Control all remote access through a limited number of managed access control points.

Applicability: All	**References:** ARS: AC-17(3); IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(3)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(3).1

Assessment Objective

Determine if:
(i) the organization defines managed access control points for remote access to the information system; and
(ii) the information system controls all remote accesses through a limited number of managed access control points.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for remote access.(Optional)

AC-17(4) – Enhancement (Moderate)

Control

Permit remote access for privileged functions only for compelling operational needs and document the rationale for such access in the security plan for the information system.

Applicability: All	**References:** ARS: AC-17(4); FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(4)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(4).1

Assessment Objective

Determine if:
(i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed; and
(ii) the organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for remote access.(Optional)

AC-17(CMS-1) – Enhancement (Moderate)

Control

Enable secure management protocols through a VPN link(s) if connected to the information system and using remote administration. Utilize an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based).

Applicability: All	**References:** ARS: AC-17(CMS-1); IRS-1075: 5.6.3.2#5	**Related Controls:** SC-13

ASSESSMENT PROCEDURE: AC-17(CMS-1).1

Assessment Objective

Determine if the organization documents, monitors, and controls all methods of remote access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if secure management protocols through a VPN link(s) if connected to the information system and using remote administration are enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if secure management protocols through a VPN link(s) if connected to the information system and using remote administration are enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system.

Test: Automated mechanisms implementing the access control policy for remote access to determine that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system.

AC-17(CMS-2) – Enhancement (Moderate)

Control

Implement password protection for remote access connections.

Applicability: All	**References:** ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(CMS-2).1

Assessment Objective

Determine if the organization documents, monitors, and controls all methods of remote access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if password protection for remote access connections is implemented.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if password protection is required for remote access connections.

Test: Automated mechanisms implementing the access control policy for remote access to determine remote access connections by attempting to gain access without a password.

AC-17(CMS-3) – Enhancement (Moderate)

Control

Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) cannot be used.

Applicability: All	**References:** ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(CMS-3).1

Assessment Objective

Determine if:

(i) the organization defines managed access control points for remote access to the information system; and

(ii) the information system controls all remote accesses through a limited number of managed access control points.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified annually.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually.

Test: Automated mechanisms implementing the access control policy for remote access to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually.

AC-17(CMS-4) – Enhancement (Moderate)

Control

If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix A for e-Authentication standards.

Applicability: All	**References:** ARS: AC-17(CMS-4); IRS-1075: 5.6.3.2#5	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(CMS-4).1

Assessment Objective

Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if e-authentication is implemented as a remote access solution or associated with remote access. If so, refer to ARS Appendix A for e-Authentication standards.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system implements e-authentication. If so, refer to ARS Appendix A for e-Authentication standards.

Test: Automated mechanisms implementing the access control policy for remote access to determine if e-authentication is implemented. If so, refer to ARS Appendix A for e-Authentication standards.

AC-17(FIS-1) – Enhancement (Moderate)

Control

Remote access phone numbers are not published and are periodically changed.

Applicability: All	**References:** FISCAM: TAC-3.2.E.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(FIS-1).1

Assessment Objective

Determine if the organization changes, periodically, remote access phone numbers and those phone numbers are not published.

Assessment Methods And Objects

Examine: Documentation showing changes to dial-in numbers.

Examine: Entity's telephone directory to verify that the numbers are not listed.

Examine: Pertinent policies and procedures.

Interview: Remote access users.

AC-18 – Wireless Access Restrictions (Moderate)

Control

Installation of wireless access points (WAP) into CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. Authorized WAP devices and wireless access shall be monitored on a regular basis, and wireless communications shall be secured through the use of approved encryption controls.

Guidance

NIST SP 800-48 and 800-97 provide guidance on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion detection and prevention.

Applicability: All	**References:** ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18	**Related Controls:**

ASSESSMENT PROCEDURE: AC-18.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for wireless technologies;
(ii) the organization authorizes, monitors, and controls wireless access to the information system; and
(iii) the wireless access restrictions are consistent with NIST SP 800-48 and 800-97.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records.

Test: Wireless access usage and restrictions.

AC-18(0) – Enhancement (Moderate)

Control

CMS policy prohibits the use of wireless access unless explicitly approved by the CMS CIO or his/her designated representative.

Applicability: All	**References:** ARS: AC-18(0); NIST 800-53/53A: AC-18; PISP: 4.1.18	**Related Controls:**

ASSESSMENT PROCEDURE: AC-18(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records.

Test: Wireless access usage and restrictions.

AC-18(1) – Enhancement (Moderate)		
Control If wireless access is explicitly approved, approved authentication and encryption is used to protect wireless access to the information system.		
Applicability: All	**References:** ARS: AC-18(1); NIST 800-53/53A: AC-18(1)	**Related Controls:**
ASSESSMENT PROCEDURE: AC-18(1).1		
Assessment Objective Determine if the organization uses authentication and encryption to protect wireless access to the information system. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test:** Automated mechanisms implementing the access control policy for wireless access to the information system.(Optional)		
AC-18(2) – Enhancement (Moderate)		
Control Perform quarterly scans for unauthorized wireless access points and take appropriate action if any access points are discovered.		
Guidance Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.		
Applicability: All	**References:** ARS: AC-18(2)	**Related Controls:**
ASSESSMENT PROCEDURE: AC-18(2).1		
Assessment Objective Determine if: (i) the organization defines the frequency of scans for unauthorized wireless access points; and (ii) the organization scans for unauthorized wireless access points in accordance with organization-defined frequency and takes appropriate action if such an access points are discovered. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records.(Optional) **Test:** Scanning procedure for unauthorized wireless access points.(Optional)		
AC-18(DIR-1) – Enhancement (Moderate)		
Control If wireless access is explicitly approved, wireless devices, service set identifier broadcasting is disabled and the following wireless access controls are implemented: (a) encryption protection is enabled; (b) access points are placed in secure areas; (c) access points are shut down when not in use (i.e., nights, weekends); (d) a firewall is implemented between the wireless network and the wired infrastructure; (e) MAC address authentication is utilized; (f) static IP addresses, not DHCP, is utilized; (g) personal firewalls are utilized on all wireless clients; (h) file sharing is disabled on all wireless clients; (i) Intrusion detection agents are deployed on the wireless side of the firewall; and (j) wireless activity is monitored and recorded, and the records are reviewed on a regular basis.		
Applicability: All	**References:**	**Related Controls:**
ASSESSMENT PROCEDURE: AC-18(DIR-1).1		
Assessment Objective Determine if the organization establishes wireless policies and strict procedures that control access to the wireless LAN and separates/restricts the wireless LAN from the wired network infrastructure. **Assessment Methods And Objects** **Examine:** Access control procedures for continuous wireless intrusion monitoring of approved and operational wireless systems. **Interview:** Staff personnel who review the wireless LAN records know what to look for in the data for an unauthorized intrusion, and the staff knows the reporting procedures when an unauthorized intrusion is detected.		

Test: The wireless LAN does not allow rogue wireless devices into the approved wireless network infrastructure.

AC-19 – Access Control for Portable and Mobile Devices (Moderate)

Control

The connection of portable and mobile devices (e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CIO or his/her designated representative. Prior to connecting portable and mobile devices to CMS information systems and networks, such devices shall be configured to comply with CMS IS policies and procedures. The storage and transmission of CMS sensitive information on portable and mobile information devices shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware. The activities and controls shall be commensurate with the system security level of the information.

Guidance

Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family.

Applicability: All	**References:** ARS: AC-19; IRS-1075: 4.6#1; NIST 800-53/53A: AC-19; PISP: 4.1.19	**Related Controls:** MP-4, MP-5

ASSESSMENT PROCEDURE: AC-19.1

Assessment Objective

Determine if:
(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;
(ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and
(iii) the organization authorizes, monitors, and controls device access to organizational information systems.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Interview: Organizational personnel who use portable and mobile devices to access the information system.
Test: Automated mechanisms implementing access control policy for portable and mobile devices.(Optional)

AC-19(CMS-1) – Enhancement (Moderate)

Control

If portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative:
Employ an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Applicability: All	**References:** ARS: AC-19(CMS-1); FISCAM: TAC-3.3; IRS-1075: 4.6#1, 4.7.2#1	**Related Controls:** MA-CMS-1, MA-CMS-2, SC-13

ASSESSMENT PROCEDURE: AC-19(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;
(ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and
(iii) the organization authorizes, monitors, and controls device access to organizational information systems.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records to determine if portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative. Also, determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.
Interview: Organizational personnel who use portable and mobile devices to access the information system to determine if portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in

writing by the CIO or his/her designated representative. Also, determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Test: Automated mechanisms implementing access control policy for portable and mobile devices to determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

AC-20 – Use of External Information Systems (Moderate)

Control

External information systems, including, but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports shall not be used to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative.

Strict terms and conditions shall be established for the use of external information systems. The terms and conditions shall address, at a minimum:
4.1.20.1. The types of applications that can be accessed from external information systems;
4.1.20.2. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
4.1.20.3. How other users of the external information system will be prevented from accessing federal information;
4.1.20.4. The use of virtual private networking (VPN) and firewall technologies;
4.1.20.5. The use of and protection against the vulnerabilities of wireless technologies;
4.1.20.6. The maintenance of adequate physical security controls;
4.1.20.7. The use of virus and spyware protection software; and
4.1.20.8. How often the security capabilities of installed software are to be updated.

Guidance

External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.
Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Applicability: All	**References:** ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20	**Related Controls:**

ASSESSMENT PROCEDURE: AC-20.1

Assessment Objective

Determine if:
(i) the organization defines the types of applications that can be accessed from the external information system;
(ii) the organization defines the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system; and
(iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel who use external information systems to access the information system.(Optional)

AC-20(1) – Enhancement (Moderate)

Control

Users are prohibited from using any external information system to access the information system or to process, store, or transmit CMS-controlled information except in situations where the organization:
(a) Can verify the employment of required security controls on the external system as specified in CMS' information security policy and the organization's system security plan; or

(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

Applicability: All	References: ARS: AC-20(1); IRS-1075: 4.7.2#1; NIST 800-53/53A: AC-20(1)	Related Controls:

ASSESSMENT PROCEDURE: AC-20(1).1

Assessment Objective

Determine if the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:
- verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization's information security policy and system security plan when allowing connections to the external information system; or
- approves, for authorized exceptions, information system connection or processing agreements with the organizational entity hosting the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; information system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records.

AC-20(CMS-1) – Enhancement (Moderate)

Control

Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.

Applicability: All	References: ARS: AC-20(CMS-1); IRS-1075: 4.7.2#1, 4.7.3#3	Related Controls:

ASSESSMENT PROCEDURE: AC-20(CMS-1).1

Assessment Objective

Determine if the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

Interview: Organizational personnel who use external information systems to access the information system to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

AC-20(PII-1) – Enhancement (Moderate)

Control

Only organization owned computers and software can be used to process, access, and store PII.

Applicability: All	References: IRS-1075: 4.7.1#1	Related Controls:

ASSESSMENT PROCEDURE: AC-20(PII-1).1

Assessment Objective

Determine if the organizational computers and software are owned by that organization that processes, accesses and stores PII.

Assessment Methods And Objects

Examine: Organizational computer and software purchase orders indicating ownership of computers and software used to process, access and store PII.

Interview: Organizational staff indicating that only organizational owned computers and software are used to process, access and store PII.

AC-CMS-1 – System Boot Access (Moderate)

Control

System boot access shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can alter or perform non-standard boots of systems and/or components of the information system shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Guidance

When a person has unrestrained physical access to any computing system or network device the person has control of the equipment.
If the person does not have the capability to locally access the information system's data though the boot process this can assist in protecting the data from loss or unauthorized access to the data.
Note: Even though the system root access may be protected by privilege access controls a miss configured system can allow the system to reboot and thus allowing a boot / access from unauthorized media. An example of this is a LINUX system, not configured correctly, when CONT+ALT+DEL is issued from the keyboard the equipment will re-boot automatically.

Applicability: All	**References:** ARS: AC-CMS-1; PISP: 4.1.21	**Related Controls:**

ASSESSMENT PROCEDURE: AC-CMS-1.1

Assessment Objective

Determine if the organization assesses the need for system boot access and if necessary controls, documents and monitors the continued need for system boot access.

Assessment Methods And Objects

Examine: System boot access documentation to determine that there is or is not a need for boot access.
Interview: Organizational personnel to determine that there is or is not a need for system boot access.

AC-CMS-1(CMS-1) – Enhancement (Moderate)

Control

If not explicitly required, boot access to removable media drives is disabled.

Applicability: All	**References:** ARS: AC-CMS-1(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-CMS-1(CMS-1).1

Assessment Objective

Determine if the organization evaluates the need for system boot access by removable media drives.

Assessment Methods And Objects

Examine: System boot access documentation to determine that, if not explicitly required, boot access to removable media drives is disabled.
Interview: Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled.
Test: Information system sample of workstations to determine if boot access to removable media drives is disabled.

AC-CMS-1(CMS-2) – Enhancement (Moderate)

Control

System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).

Applicability: All	**References:** ARS: AC-CMS-1(CMS-2)	**Related Controls:** IA-5

ASSESSMENT PROCEDURE: AC-CMS-1(CMS-2).1

Assessment Objective

Determine if the organization controls access to the system BIOS when unauthorized personnel may be in physical proximity to the system.

Assessment Methods And Objects

Examine: System BIOS documentation to determine if System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).
Interview: Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled.
Test: Information system sample of workstations by attempting to access the System BIOS. Ensure that access to the System BIOS is protected by password.

AC-CMS-1(CMS-3) – Enhancement (Moderate)

Control

If not explicitly required, removable media drive functionality is disabled.

Applicability: All	**References:** ARS: AC-CMS-1(CMS-3)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-CMS-1(CMS-3).1

Assessment Objective

Determine if the organization disables removable media drive functionality If not explicitly required.

Assessment Methods And Objects

Examine: Removable media drive documentation to determine that, if not explicitly required, removable media drive functionality is disabled.
Interview: Organizational personnel to determine that, if not explicitly required, removable media drive functionality is disabled.
Test: Sample of Information system workstations to determine if removable media drive functionality is disabled.

Awareness and Training (AT) – *Operational*

AT-1 – Security Awareness and Training Policy and Procedures (Moderate)

Control

An IS AT program shall be developed, documented, and implemented effectively for all personnel, including contractors and any other users of CMS information and information systems. The IS AT program shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information, information systems, and networks.

Guidance

The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-16 and 800-50 provide guidance on security awareness and training. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AT-1; FISCAM: TSP-4.2.2; IRS-1075: 5.6.2.7#1.1-2, 6.1#1; NIST 800-53/53A: AT-1; PISP: 4.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AT-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security awareness and training policy and procedures;
(ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review security awareness and training policy and procedures; and
(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.
Interview: Organizational personnel with security awareness and training responsibilities.(Optional)

ASSESSMENT PROCEDURE: AT-1.2

Assessment Objective

Determine if:
(i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.
Interview: Organizational personnel with security awareness and training responsibilities.(Optional)

AT-2 – Security Awareness (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS AT program shall be consistent with 5 CFR Part 930 (http://opm.gov/fedregis/2004/69-061404-32835-a.pdf) and the guidance provided in NIST SP 800-50.

Guidance

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	**References:** ARS: AT-2; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3; NIST 800-53/53A: AT-2; PISP: 4.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2.1

Assessment Objective

Determine if:

(i) the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes;
(ii) the security awareness training is consistent with applicable regulations and NIST SP 800-50;
(iii) the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access;
(iv) the organization defines the frequency of refresher security awareness training; and
(v) the organization provides refresher security awareness training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan; other relevant documents or records.
Interview: Organizational personnel comprising the general information system user community.(Optional)

AT-2(0) – Enhancement (Moderate)

Control

All information system users (including managers and senior executives) receive basic information security awareness training prior to accessing any system's information; when required by system changes; and every 365 days thereafter.

Applicability: All	**References:** ARS: AT-2(0); FISCAM: TSP-3.3.1; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3, 6.2#1.1-2, 6.2#1.4, 6.2#2.1; NIST 800-53/53A: AT-2; PISP: 4.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan (for organization-defined frequency of refresher security awareness training); other relevant documents or records.

AT-2(CMS-1) – Enhancement (Moderate)

Control

Establish a program to promote continuing awareness of information security issues and threats.

Applicability: All	**References:** ARS: AT-2(CMS-1); HIPAA: 164.308(a)(5)(ii)(A); IRS-1075: 5.6.2.7#1.3	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2(CMS-1).1

Assessment Objective

Determine if the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records to determine that a program to promote continuing awareness of information security issues and threats has been established.
Interview: Organizational personnel with security awareness and training responsibilities to determine that a program to promote continuing awareness of information security issues and threats has been established.

AT-3 – Security Training (Moderate)

Control

The organization shall identify and document all positions and/or roles with significant information system security responsibilities during the system development life cycle. All personnel with significant information system security responsibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Content of the security awareness training shall be determined based upon the information systems to which personnel have authorized access. The employee shall acknowledge having received the security and awareness training either in writing or electronically as part of the training course completion.

Guidance

The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	**References:** ARS: AT-3; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: AT-3.1

Assessment Objective

Determine if:
(i) the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities;
(ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes;
(iii) the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security;
(iv) the security training is consistent with applicable regulations and NIST SP 800-50;
(v) the organization defines the frequency of refresher security training; and
(vi) the organization provides refresher security training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan; other relevant documents or records.
Interview: Organizational personnel with significant information system security responsibilities.(Optional)

AT-3(0) – Enhancement (Moderate)

Control

Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to CMS networks, systems, and/or applications; when required by system changes; and refresher training every 365 days thereafter.

Applicability: All	**References:** ARS: AT-3(0); FISCAM: TSP-3.3.1; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: AT-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan (for organization-defined frequency of refresher security training); other relevant documents or records.

AT-4 – Security Training Records (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that individual IS training activities, including basic security awareness training and specific information system security training, are properly documented and monitored.

Guidance

Procedures and training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.
(2) Executives must receive training in information security basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	References: ARS: AT-4; FISCAM: TSP-4.2.3; IRS-1075: 6.2#1.3; NIST 800-53/53A: AT-4; PISP: 4.2.4	Related Controls:

ASSESSMENT PROCEDURE: AT-4.1

Assessment Objective

Determine if the organization monitors and documents basic security awareness training and specific information system security training.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.

AT-5 – Contacts with Security Groups and Associations (Moderate)

Control

Contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations shall be encouraged and supported to enable security personnel to stay up to date with the latest recommended security practices, techniques, and technologies; and to share the latest security-related information including threats, vulnerabilities, and incidents.

Guidance

To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Applicability: All	References: ARS: AT-5; HSPD 7: H(25); NIST 800-53/53A: AT-5; PISP: 4.2.5	Related Controls:

ASSESSMENT PROCEDURE: AT-5.1

Assessment Objective

Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security techniques and technologies and to share security-related information.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records.(Optional)

Audit and Accountability (AU) – *Technical*

AU-1 – Audit and Accountability Policy and Procedures (Moderate)

Control

All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the implementation and management of audit controls, and shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AU-1; IRS-1075: 5.6.3.3#1; NIST 800-53/53A: AU-1; PISP: 4.3.1	**Related Controls:**

ASSESSMENT PROCEDURE: AU-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents audit and accountability policy and procedures;
(ii) the organization disseminates audit and accountability policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review audit and accountability policy and procedures; and
(iv) the organization updates audit and accountability policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Audit and accountability policy and procedures; other relevant documents or records.
Interview: Organizational personnel with audit and accountability responsibilities.(Optional)

ASSESSMENT PROCEDURE: AU-1.2

Assessment Objective

Determine if:
(i) the audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Audit and accountability policy and procedures; other relevant documents or records.
Interview: Organizational personnel with audit and accountability responsibilities.(Optional)

AU-2 – Auditable Events (Moderate)

Control

Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security incidents. The selection of auditable events shall be based upon a risk assessment as to which events require auditing on a continuous basis, and which events require auditing in response to specific situations.

Guidance

The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**References:** ARS: AU-2; FISCAM: TAC-4.3.4, TSD-3.2.2; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2; PISP: 4.3.2	**Related Controls:** AU-4

ASSESSMENT PROCEDURE: AU-2.1

Assessment Objective

Determine if:
(i) the organization defines information system auditable events;
(ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and
(iii) the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing information system auditing of organization-defined auditable events.(Optional)

AU-2(0) – Enhancement (Moderate)

Control

Generate audit records for the following events:
(a) User account management activities,
(b) System shutdown,
(c) System reboot,
(d) System errors,
(e) Application shutdown,
(f) Application restart,
(g) Application errors,
(h) File creation,
(i) File deletion,
(j) File modification,
(k) Failed and successful log-ons,
(l) Security policy modifications, and
(m) Use of administrator privileges.

Guidance

Note: For FTI, generate audit records for the following events in addition to those specified in other controls:
(a) All successful and unsuccessful authorization attempts.
(b) All changes to logical access control authorities (e.g., rights, permissions).
(c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
(d) The audit trail shall capture the enabling or disabling of audit report generation services.
(e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

Applicability: All	**References:** ARS: AU-2(0); FISCAM: TAC-2.1.5, TAC-4.1, TSD-3.2.4; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3; NIST 800-53/53A: AU-2; PISP: 4.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AU-2(1) – Enhancement (Moderate)

Control

Provide the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical) time correlated audit trail.

Applicability: All	**References:** ARS: AU-2(1); IRS-1075: 5.6.3.3#2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(1).1

Assessment Objective

Determine if:
(i) the organization defines the components of the information system that generate audit records; and

(ii) the information system compiles audit records from the organization-defined (multiple) components within the information system into a systemwide (logical or physical), time-correlated audit trail.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing a system-wide auditing capability.(Optional)

AU-2(2) – Enhancement (Moderate)

Control

Provide the capability to manage the selection of events to be audited by individual components of the information system.

Applicability: All	**References:** ARS: AU-2(2); IRS-1075: 5.6.3.3#2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(2).1

Assessment Objective

Determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing Information system auditing for the specified components of the information system.(Optional)

AU-2(3) – Enhancement (Moderate)

Control

Periodically review and update the list of auditable events.

Applicability: All	**References:** ARS: AU-2(3); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2(3)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(3).1

Assessment Objective

Determine if the organization periodically reviews and updates the list of organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records.

Interview: Organizational personnel with auditing and accountability responsibilities.(Optional)

AU-2(CMS-1) – Enhancement (Moderate)

Control

Enable logging for perimeter devices, including firewalls and routers.
(a) Log packet screening denials originating from un-trusted networks,
(b) Packet screening denials originating from trusted networks,
(c) User account management,
(d) Modification of proxy services,
(e) Application errors,
(f) System shutdown and reboot,
(g) System errors,
(h) Modification of proxy services, and
(i) Modification of packet filters.

Applicability: All	**References:** ARS: AU-2(CMS-1); HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines information system auditable events;
(ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and
(iii) the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if logging-on is enabled for perimeter devices, including firewalls and routers. This logging will capture the following information:
(a) Log packet screening denials originating from un-trusted networks,
(b) packet screening denials originating from trusted networks,
(c) user account management,
(d) modification of proxy services,
(e) application errors,
(f) system shutdown and reboot,
(g) system errors,
(h) modification of proxy services, and
(i) modification of packet filters.

Interview: Organizational personnel with audit and accountability responsibilities to determine if logging-on is enabled for perimeter devices, including firewalls and routers. This logging will capture the following information:
(a) Log packet screening denials originating from un-trusted networks,
(b) packet screening denials originating from trusted networks,
(c) user account management,
(d) modification of proxy services,
(e) application errors,
(f) system shutdown and reboot,
(g) system errors,
(h) modification of proxy services, and
(i) modification of packet filters.

Test: Automated mechanisms implementing information system auditing of organization-defined auditable events.

AU-2(CMS-2) – Enhancement (Moderate)

Control

Verify that proper logging is enabled in order to audit administrator activities.

Applicability: All	**References:** ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(CMS-2).1

Assessment Objective

Determine if the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if proper logging is enabled in order to audit administrator activities.

Interview: Organizational personnel with account audit and accountability responsibilities to determine if proper logging is enabled in order to audit administrator activities.

Test: Automated mechanisms implementing information system auditing of organization-defined auditable events.

AU-3 – Content of Audit Records (Moderate)

Control

Automated mechanisms shall be established to provide the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome.

Guidance

Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**References:** ARS: AU-3; FISCAM: TAC-3.2.D.1, TAN-2.1.9; IRS-1075: 5.6.3.3#3; NIST 800-53/53A: AU-3; PISP: 4.3.3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-3.1

Assessment Objective

Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records.

Test: Automated mechanisms implementing information system auditing of auditable events.(Optional)

AU-3(1) – Enhancement (Moderate)

Control

Provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

Applicability: All	**References:** ARS: AU-3(1); NIST 800-53/53A: AU-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-3(1).1

Assessment Objective

Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject.(Optional)

AU-3(CMS-1) – Enhancement (Moderate)

Control

Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still required.

Applicability: All	**References:** ARS: AU-3(CMS-1); FISCAM: TAC-4.1; HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AU-3(CMS-1).1

Assessment Objective

Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing the content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records to determine if the organization records disclosures of sensitive information, including protected health and financial information. The organization must log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still required.

Interview: Organizational personnel with account audit and accountability responsibilities to determine if the organization records disclosures of sensitive information, including protected health and financial information. The organization must log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still required.

Test: Automated mechanisms implementing information system auditing of auditable events with organization-defined audit record content.

AU-4 – Audit Storage Capacity (Moderate)

Control

A sufficient amount of information system storage capacity shall be allocated for audit records, and information systems shall be configured to reduce the likelihood of audit records exceeding such storage capacity.

Guidance

The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements.

Applicability: All	**References:** ARS: AU-4; IRS-1075: 5.6.3.3#4; NIST 800-53/53A: AU-4; PISP: 4.3.4	**Related Controls:** AU-2, AU-5, AU-6, AU-7, SI-4

ASSESSMENT PROCEDURE: AU-4.1

Assessment Objective

Determine if:

(i) the organization defines audit record storage capacity for the information system components that generate audit records; and

(ii) the organization establishes information system configuration settings to reduce the likelihood of the audit record storage capacity being exceeded.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components generating audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AU-5 – Response to Audit Processing Failures (Moderate)

Control

Automated mechanisms shall be established which provide the capability to generate information system alerts for appropriate officials in the event of an audit failure or audit storage capacity being reached and to take appropriate additional actions.

Guidance

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Applicability: All	References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5	Related Controls: AU-4

ASSESSMENT PROCEDURE: AU-5.1

Assessment Objective

Determine if:
(i) the organization defines actions to be taken in the event of an audit processing failure;
(ii) the organization defines personnel to be notified in case of an audit processing failure; and
(iii) the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure or audit storage capacity being reached.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system response to audit processing failures.(Optional)

AU-5(0) – Enhancement (Moderate)

Control

Alert appropriate officials and take the following actions in response to an audit failure or audit storage capacity issue:
(a) Shutdown the information system,
(b) Stop generating audit records, or
(c) Overwrite the oldest records, in the case that storage media is unavailable.

Applicability: All	References: ARS: AU-5(0); NIST 800-53/53A: AU-5; PISP: 4.3.5	Related Controls:

ASSESSMENT PROCEDURE: AU-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for list of actions to be taken by the information system in case of an audit processing failure); information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

AU-6 – Audit Monitoring, Analysis, and Reporting (Moderate)

Control

Information system audit records shall be reviewed and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and/or suspicious activity. Such activity shall be investigated and reported to appropriate officials, in accordance with current CMS Procedures.

Guidance

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Applicability: All	References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6	Related Controls: AU-4, IR-4

ASSESSMENT PROCEDURE: AU-6.1

Assessment Objective

Determine if:
(i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity;
(ii) the organization investigates suspicious activity or suspected violations;
(iii) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and
(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records.
Test: Information system audit monitoring, analysis, and reporting capability.(Optional)

ASSESSMENT PROCEDURE: AU-6.2

Assessment Objective

Determine if the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Interview: Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities.(Optional)

AU-6(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Applicability: All	**References:** ARS: AU-6(1); HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Automated mechanisms integrating audit monitoring, analysis, and reporting into an organizational process for investigation and response to suspicious activities.(Optional)

AU-6(2) – Enhancement (Moderate)

Control

Employ automated mechanisms to immediately alert security personnel of the following minimal examples of inappropriate or unusual activities with security implications: threats to infrastructure, systems or assets; threats to CMS sensitive data; and threats to finances, personnel, or property.

Applicability: All	**References:** ARS: AU-6(2); HIPAA: 164.312(b); NIST 800-53/53A: AU-6(2)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(2).1

Assessment Objective

Determine if:
(i) the organization defines inappropriate or unusual activities with security implications; and
(ii) the organization employs automated mechanisms to alert security personnel of the occurrence of any organization-defined inappropriate or unusual activities with security implications.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing security alerts.

AU-6(CMS-1) – Enhancement (Moderate)

Control

Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than

once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Applicability: All	References: ARS: AU-6(CMS-1); FISCAM: TAC-4.2	Related Controls:

ASSESSMENT PROCEDURE: AU-6(CMS-1).1

Assessment Objective

Determine if:
(i) the organization regularly reviews / analyzes audit records for indications of inappropriate or unusual activity;
(ii) the organization investigates suspicious activity or suspected violations;
(iii) the organization reports findings of inappropriate/usual activities, suspicious behavior, or suspected violations to appropriate officials; and
(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Interview: Organizational personnel responsible for audit and accountability to determine if initialization sequences, log-ons and errors; system processes and performance; and system resource utilization are recorded to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Test: Information system audit monitoring, analysis, and reporting capability to determine if initialization sequences, log-ons and errors; system processes and performance; and system resource utilization are recorded to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

AU-6(CMS-2) – Enhancement (Moderate)

Control

Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Applicability: All	References: ARS: AU-6(CMS-2)	Related Controls:

ASSESSMENT PROCEDURE: AU-6(CMS-2).1

Assessment Objective

Determine if the organization regularly reviews / analyzes audit records for indications of inappropriate or unusual activity.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Interview: Organizational personnel responsible for audit and accountability to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Test: Information system audit monitoring, analysis, and reporting capability to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

AU-6(CMS-3) – Enhancement (Moderate)

Control

Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.

Applicability: All	References: ARS: AU-6(CMS-3); FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.3, TAC-4.3.4; HIPAA: 164.312(b)	Related Controls:

ASSESSMENT PROCEDURE: AU-6(CMS-3).1

Assessment Objective

Determine if the organization investigates suspicious activity or suspected violations.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.

Interview: Organizational personnel responsible for audit and accountability to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.

Test: Information system audit monitoring, analysis, and reporting capability to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.

AU-6(CMS-4) – Enhancement (Moderate)

Control

Use automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior.

Applicability: All	**References:** ARS: AU-6(CMS-4); HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-4).1

Assessment Objective

Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

Interview: Organizational personnel responsible for audit and accountability to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

Test: Information system audit monitoring, analysis, and reporting capability to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

AU-6(CMS-5) – Enhancement (Moderate)

Control

Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.

Applicability: All	**References:** ARS: AU-6(CMS-5); FISCAM: TAC-2.1.5; HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-5).1

Assessment Objective

Determine if the organization monitors activities of system administrators.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Interview: Organizational personnel with audit and accountability responsibilities to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Test: Information system audit monitoring, analysis, and reporting capability to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

AU-6(CMS-6) – Enhancement (Moderate)

Control

Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Applicability: All	**References:** ARS: AU-6(CMS-6); HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-6).1

Assessment Objective

Determine if the organization randomly performs a manual review of automated audit systems to validate the correctness of the automated system.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Interview: Organizational personnel with audit and accountability responsibilities to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Test: Information system audit monitoring, analysis, and reporting capability to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

AU-6(FIS-1) – Enhancement (Moderate)		
Control The use of privileged system software and utilities is reviewed by technical management. Systems programmers' activities are monitored and reviewed. Inappropriate or unusual activity in using utilities is investigated.		
Applicability: All	**References:** FISCAM: TSS-2.2.1, TSS-2.2.2, TSS-2.2.3	**Related Controls:**
ASSESSMENT PROCEDURE: AU-6(FIS-1).1		
Assessment Objective Determine if the organization monitors and reviews system programmers' activities and investigates inappropriate or unusual activities when using privileged system software utilities. **Assessment Methods And Objects** **Examine:** Documentation supporting the supervising and monitoring of systems programmers' activities. **Examine:** Documentation supporting their reviews. **Examine:** Documentation supporting these investigations. **Examine:** Pertinent policies and procedures. **Interview:** Systems programmer supervisors to determine their activities related to supervising and monitoring their staff. **Interview:** Technical management regarding their reviews of privileged system software and utilities usage.		
AU-6(IRS-1) – Enhancement (Moderate)		
Control For FTI, all requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log. (see IRS Pub. 1075, sect 6.3.1)		
Applicability: All	**References:** IRS-1075: 6.3.1#1	**Related Controls:**
ASSESSMENT PROCEDURE: AU-6(IRS-1).1		
Assessment Objective Determine if the organization maintains a log for all requests for returned FTI, and the log includes receipt and/or disposal of returns (see IRS Pub. 1075, sect 6.3.1). **Assessment Methods And Objects** **Examine:** Logs for requests of FTI include receipt and/or disposal or FTI information is returned. **Interview:** Responsible organizational staff handling FTI to determine is there is an effective log of FTI requests, disposal or returns.		
AU-7 – Audit Reduction and Report Generation (Moderate)		
Control Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to enable human review of audit information and the generation of appropriate audit reports.		
Guidance Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.		
Applicability: All	**References:** ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7	**Related Controls:** AU-4
ASSESSMENT PROCEDURE: AU-7.1		
Assessment Objective Determine if the information system provides an audit reduction and report generation capability. **Assessment Methods And Objects** **Examine:** Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities.(Optional) **Test:** Audit reduction and report generation capability.		
AU-7(1) – Enhancement (Moderate)		
Control Employ a system capability that automatically processes audit records for events of interest based upon selectable, event criteria.		
Applicability: All	**References:** ARS: AU-7(1); NIST 800-53/53A: AU-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-7(1).1

Assessment Objective

Determine if the information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records.

Test: Audit reduction and report generation capability.(Optional)

AU-8 – Time Stamps (Moderate)

Control

Audit records shall employ time stamps for use in audit record generation. Time stamps of audit records shall be generated using internal system clocks that are synchronized system-wide.

Guidance

Time stamps (including date and time) of audit records are generated using internal system clocks.

Applicability: All	**References:** ARS: AU-8; NIST 800-53/53A: AU-8; PISP: 4.3.8	**Related Controls:**

ASSESSMENT PROCEDURE: AU-8.1

Assessment Objective

Determine if the information system provides time stamps for use in audit record generation.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing time stamp generation.

AU-8(1) – Enhancement (Moderate)

Control

Information system clock synchronization occurs daily and at system boot.

Applicability: All	**References:** ARS: AU-8(1); NIST 800-53/53A: AU-8(1)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-8(1).1

Assessment Objective

Determine if:

(i) the organization defines the frequency of internal clock synchronization for the information system; and

(ii) the organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing time stamp generation; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing internal information system clock synchronization.(Optional)

AU-9 – Protection of Audit Information (Moderate)

Control

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

Guidance

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Applicability: All	**References:** ARS: AU-9; NIST 800-53/53A: AU-9; PISP: 4.3.9	**Related Controls:**

ASSESSMENT PROCEDURE: AU-9.1

Assessment Objective

Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records.

Test: Automated mechanisms implementing audit information protection.(Optional)

AU-10 – Non-Repudiation (Moderate)

Control

Non-repudiation mechanisms shall be implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message.

Guidance

Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Applicability: All	**References:** ARS: AU-10; NIST 800-53/53A: AU-10; PISP: 4.3.10	**Related Controls:**

ASSESSMENT PROCEDURE: AU-10.1

Assessment Objective

Determine if the information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing non-repudiation capability.(Optional)

AU-11 – Audit Record Retention (Moderate)

Control

Audit records shall be retained to provide support for after-the-fact investigations of security incidents, and to meet regulatory and/or CMS information retention requirements. The National Archives and Records Administration maintains criteria for record retention across many disciplines and information security retention standards shall not be construed to relieve or waive these other standards.

Guidance

The organization retains audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions (CMS sensitive information retention). Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST SP 800-61 provides guidance on computer security incident handling and audit record retention.

Applicability: All	**References:** NIST 800-53/53A: AU-11	**Related Controls:**

ASSESSMENT PROCEDURE: AU-11.1

Assessment Objective

Determine if:

(i) the organization defines the retention period for audit records generated by the information system; and

(ii) the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information system audit record retention responsibilities.(Optional)

AU-11(0) – Enhancement (Moderate)

Control

Retain audit records for ninety (90) days, and archive old audit records. Retain audit record archives for one (1) year.

Applicability: All	**References:** ARS: AU-11(0); NIST 800-53/53A: AU-11; PISP: 4.3.11	**Related Controls:**

ASSESSMENT PROCEDURE: AU-11(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information system audit record retention responsibilities.(Optional)

AU-11(PII-1) – Enhancement (Moderate)

Control

Employ mechanisms to facilitate the review of PII disclosure/access records and retain the records for five (5) years or the applicable records control schedule, whichever is longer.

Applicability: All	**References:** IRS-1075: 3.1#1	**Related Controls:**

ASSESSMENT PROCEDURE: AU-11(PII-1).1

Assessment Objective

Determine if the organization employs mechanisms to facilitate the review of PII disclosures/access records and retains the records for five (5) years or the applicable records control schedule, whichever is longer.

Assessment Methods And Objects

Examine: PII disclosure/access audit records are retained or a control schedule indicates (5) five years or longer.

AU-11(PII-2) – Enhancement (Moderate)

Control

To support the audit of activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever PII is stored.

Applicability: All	**References:** IRS-1075: 5.6.3.3#5.2	**Related Controls:**

ASSESSMENT PROCEDURE: AU-11(PII-2).1

Assessment Objective

Determine if the organization ensures that audit information is archived for six (6) years to enable the recreation of computer related accesses to both the operation system and the application wherever PII is stored.

Assessment Methods And Objects

Examine: PII audit information is retained for (6) six years to enable recreation of computer related access to both the operation system and the application wherever PII is stored.

AU-11(PII-3) – Enhancement (Moderate)

Control

For PII, inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.

Applicability: All	**References:** IRS-1075: 6.3.5#3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-11(PII-3).1

Assessment Objective

Determine if the organizational PII inspection reports include a record of corrective actions, which is retained for a minimum of three (3) years from the date the inspection was completed.

Assessment Methods And Objects

Examine: PII inspection records to determine inclusion of corrective actions and are retained for a minimum of three (3) years from the inspection completion date.

Certification, Accreditation, and Security Assessments (CA) – *Management*

CA-1 – Certification, Accreditation, and Security Assessments Policies and Procedures (Moderate)

Control

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the Business Owner and accredited by the CMS CIO or his/her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the confidentiality, integrity, and availability (CIA) of CMS information and information systems. All C&A and security assessment activities shall be conducted in accordance with current CMS Procedures.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs, MAs, and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and/or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.4.6, Security Accreditation (CA-6).

If the CMS CIO or his/her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his/her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his/her designated representatives.

As part of the system certification and accreditation (C&A), an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, IS Risk Assessment (RA), System Security Plan (SSP), independent system tests and evaluations, the Business Owner and System Developer / Maintainer shall certify that the system meets the security requirements to the extent necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CMS CIO or the Designated Accrediting Authority (DAA).

Guidance

The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CA-1; FISCAM: TSP-5.1.2; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 5.6.1.4#1.1-2; NIST 800-53/53A: CA-1; PISP: 4.4.1	**Related Controls:** CA-6

ASSESSMENT PROCEDURE: CA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security assessment and certification and accreditation policies and procedures;
(ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review policy and procedures; and
(iv) the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.
Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.(Optional)

ASSESSMENT PROCEDURE: CA-1.2

Assessment Objective

Determine if:
(i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.

Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.(Optional)

CA-2 – Security Assessments (Moderate)

Control

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application, and comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Routine assessments shall be conducted every 365 days, in accordance with NIST SP 800-53 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST SP 800-53 A provides guidance on security control assessments to include reuse of existing assessment results.

Applicability: All	**References:** ARS: CA-2; FISCAM: TSP-5.1.1; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1; NIST 800-53/53A: CA-2; PISP: 4.4.2	**Related Controls:** CA-4, CA-6, CA-7, CA-7(1), SA-11, SI-2

ASSESSMENT PROCEDURE: CA-2.1

Assessment Objective

Determine if:

(i) the information system is in the inventory of major information systems; and

(ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security assessment policy; procedures addressing security assessments; information system security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records.

CA-3 – Information System Connections (Moderate)

Control

Management shall authorize in writing through the use of system connection agreements all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system connections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

Guidance

Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST SP 800-47 provides guidance on connecting information systems.

Applicability: All	**References:** ARS: CA-3; HSPD 7: F(19); NIST 800-53/53A: CA-3; PISP: 4.4.3	**Related Controls:** SA-9, SC-7

ASSESSMENT PROCEDURE: CA-3.1

Assessment Objective

Determine if:

(i) the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary);

(ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements;
(iii) the organization monitors/controls the system interconnections on an ongoing basis; and
(iv) information system connection agreements are consistent with NIST SP 800-47.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements.(Optional)

CA-3(CMS-1) – Enhancement (Moderate)

Control

Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

Applicability: All	**References:** ARS: CA-3(CMS-1); FISCAM: TAC-2.1.3; HSPD 7: F(19)	**Related Controls:**

ASSESSMENT PROCEDURE: CA-3(CMS-1).1

Assessment Objective

Determine if the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.
Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

CA-4 – Security Certification (Moderate)

Control

Business owners shall conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification process shall be integrated into and span across the SDLC. In addition, the Business Owner shall review the certification documentation every 365 days, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his/her designated representative.

Guidance

A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation.

Applicability: All	**References:** ARS: CA-4; FISCAM: TSS-2.2.4; HSPD 7: F(19); IRS-1075: 6.3#1.1-2; NIST 800-53/53A: CA-4; PISP: 4.4.4	**Related Controls:** CA-2, CA-6, CA-7, SA-11, SI-2

ASSESSMENT PROCEDURE: CA-4.1

Assessment Objective

Determine if:
(i) the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and
(ii) the organization employs a security certification process in accordance with OMB policy and NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with security certification responsibilities.(Optional)

CA-4(1) – Enhancement (Moderate)

Control

Employ an independent certification agent or certification team to conduct an assessment of the information system security controls.

Guidance

An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment of the security controls be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

Applicability: All	**References:** ARS: CA-4(1); HSPD 7: F(19); NIST 800-53/53A: CA-4(1)	**Related Controls:** AC-9

ASSESSMENT PROCEDURE: CA-4(1).1

Assessment Objective

Determine if the organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; security accreditation package (including information system security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.

CA-4(CMS-1) – Enhancement (Moderate)

Control

Document the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures.

Applicability: All	**References:** ARS: CA-4(CMS-1); HSPD 7: F(19), G(24)	**Related Controls:**

ASSESSMENT PROCEDURE: CA-4(CMS-1).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.

Interview: Organizational personnel with security certification responsibilities to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.

CA-5 – Plan of Action and Milestones (POA&M) (Moderate)

Control

A POA&M shall be developed, implemented, and updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M shall document the planned, implemented, and evaluated corrective actions to repair deficiencies discovered during the security control assessment, and to reduce or eliminate any known vulnerability in the information system.

Personnel shall be designated to assign, track, and update risk mitigation efforts. Designated personnel shall define and authorize corrective action plans, and monitor corrective action progress.

Guidance

The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems. NIST SP 800-30 provides guidance on risk mitigation.

Applicability: All	**References:** ARS: CA-5; FISCAM: TSP-5.2; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4; NIST 800-53/53A: CA-5; PISP: 4.4.5	**Related Controls:** CA-7

ASSESSMENT PROCEDURE: CA-5.1

Assessment Objective

Determine if:
(i) the organization develops and updates at the organization-defined frequency, a plan of action and milestones for the information system; and
(ii) the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing plan of action and milestones; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.(Optional)

CA-5(0) – Enhancement (Moderate)

Control

Develop and submit a plan of action and milestones (POA&M) for any documented information system security finding within thirty (30) days of the final results for every internal / external audit / review or test (e.g., ST&E, penetration test). Update the POA&M monthly until all the findings are resolved.

Applicability: All	**References:** ARS: CA-5(0); HSPD 7: F(19), G(24); NIST 800-53/53A: CA-5; PISP: 4.4.5	**Related Controls:**

ASSESSMENT PROCEDURE: CA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Certification and accreditation policy and procedures; information system security plan (for organization-defined frequency of plan of action and milestones updates); security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.(Optional)

CA-6 – Security Accreditation (Moderate)

Control

Explicit authorization to operate the information system shall be received from the CMS CIO or his/her designated representative prior to the system being placed into operations. If the authorization is an interim approval to operate, then the authorization shall be granted based on the designated security category of the information system. An explicit corrective action plan shall be developed, implemented effectively, and monitored by the authorizing official. Re-authorization shall be obtained prior to continued operation:
4.4.6.1. At least every three (3) years;
4.4.6.2. When substantial changes are made to the system;
4.4.6.3. When changes in requirements result in the need to process data of a higher sensitivity;
4.4.6.4. When changes occur to authorizing legislation or federal requirements;
4.4.6.5. After the occurrence of a serious security violation which raises questions about the validity of an earlier certification; and
4.4.6.6. Prior to expiration of a previous accreditation.

Guidance

OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three (3) year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems.

Applicability: All	**References:** ARS: CA-6; FISCAM: TSP-5.1.3, TSP-5.2; HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6	**Related Controls:** CA-1, CA-2, CA-4, CA-7

ASSESSMENT PROCEDURE: CA-6.1

Assessment Objective

Determine if:

(i) the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization in accordance with organization-defined frequency, at least every three (3) years;
(ii) a senior organizational official signs and approves the security accreditation;
(iii) the security accreditation process employed by the organization is consistent with NIST SP 800-37; and
(iv) the organization updates the authorization when there is a significant change to the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST SP 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.
Interview: Organizational personnel with security accreditation responsibilities.(Optional)

CA-6(0) – Enhancement (Moderate)

Control

Information systems can only be accredited for a maximum period of three (3) years, after which the information system must be re-accredited.

Applicability: All	**References:** ARS: CA-6(0); HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6	**Related Controls:**

ASSESSMENT PROCEDURE: CA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST SP 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.

CA-7 – Continuous Monitoring (Moderate)

Control

Security controls in CMS information systems shall be monitored on an on-going basis. Selection criteria for control monitoring shall be established and a subset of the security controls employed within information systems shall be selected for continuous monitoring purposes.

Guidance

Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2).
This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST SP 800-37 provides guidance on the continuous monitoring process. NIST SP 800-53 A provides guidance on the assessment of security controls.

Applicability: All	**References:** ARS: CA-7; HSPD 7: F(19); NIST 800-53/53A: CA-7; PISP: 4.4.7	**Related Controls:** CA-2, CA-4, CA-5, CA-6, CM-4, SI-2

ASSESSMENT PROCEDURE: CA-7.1

Assessment Objective

Determine if:
(i) the organization monitors the security controls in the information system on an ongoing basis; and
(ii) the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with continuous monitoring responsibilities.(Optional)

ASSESSMENT PROCEDURE: CA-7.2

Assessment Objective

Determine if:
(i) the organization conducts security impact analyses on changes to the information system;
(ii) the organization documents and reports changes to or deficiencies in the security controls employed in the information system; and
(iii) the organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with continuous monitoring responsibilities.(Optional)

CA-7(1) – Enhancement (Moderate)

Control

The use of independent certification agents or teams is not required but, if the organization uses an independent certification agent or certification team to monitor the security controls in the information system on an on-going basis, this can be used to satisfy ST&E requirements.

Guidance

The use of independent certification agents or teams is not required but, if used by the organization to monitor the security controls in the information system on an on-going basis, this can be used to satisfy ST&E requirements.

Applicability: All	**References:** ARS: CA-7(1); HSPD 7: F(19); NIST 800-53/53A: CA-7(1)	**Related Controls:** AC-9, CA-2

ASSESSMENT PROCEDURE: CA-7(1).1

Assessment Objective

Determine if the organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.(Optional)
Interview: Organizational personnel with continuous monitoring responsibilities.(Optional)

CA-7(CMS-1) – Enhancement (Moderate)

Control

Continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and
(e) Status reporting.

Applicability: All	**References:** ARS: CA-7(CMS-1); HSPD 7: F(19)	**Related Controls:**

ASSESSMENT PROCEDURE: CA-7(CMS-1).1

Assessment Objective

Determine if:
(i) the organization monitors the security controls in the information system on an ongoing basis; and
(ii) the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records to determine continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and

(e) Status reporting.
Interview: Organizational personnel with continuous monitoring responsibilities to determine continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and
(e) Status reporting.

Configuration Management (CM) – *Operational*

CM-1 – Configuration Management Policy and Procedures (Moderate)

Control

A CM process that includes the approval, testing, implementation, and documentation of changes shall be developed, documented, and implemented effectively to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with the organization's information technology architecture plans. Formally documented CM roles, responsibilities, procedures, and documentation shall be in place.

Guidance

The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CM-1; FISCAM: TCC-2.1.9, TCC-3.2.1, TCC-3.2.2, TCC-3.3.1, TSS-3.1.1, TSS-3.1.2, TSS-3.1.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-1; PISP: 4.5.1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents configuration management policy and procedures;
(ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review configuration management policy and procedures; and
(iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.
Interview: Organizational personnel with configuration management and control responsibilities.(Optional)

ASSESSMENT PROCEDURE: CM-1.2

Assessment Objective

Determine if:
(i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.
Interview: Organizational personnel with configuration management and control responsibilities.(Optional)

CM-2 – Baseline Configuration (Moderate)

Control

A baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system shall be developed and documented. Procedures shall be developed, documented, and implemented effectively to maintain the baseline configuration. The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture.

Guidance

This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture.

Applicability: All	**References:** ARS: CM-2; HIPAA: 164.310(b); NIST 800-53/53A: CM-2; PISP: 4.5.2	**Related Controls:** CM-6, CM-8

ASSESSMENT PROCEDURE: CM-2.1

Assessment Objective

Determine if:
(i) the organization develops, documents, and maintains a baseline configuration of the information system;

(ii) the baseline configuration shows relationships among information system components and is consistent with the Federal Enterprise Architecture;
(iii) the baseline configuration provides the organization with a well-defined and documented specification to which the information system is built; and
(iv) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.

CM-2(1) – Enhancement (Moderate)

Control

Update the baseline configuration of the information system as an integral part of information system component installations.

Applicability: All	**References:** ARS: CM-2(1); NIST 800-53/53A: CM-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CM-2(1).1

Assessment Objective

Determine if:
(i) the organization identifies the frequency of updates to the baseline configuration and instances that trigger configuration updates; and
(ii) the organization updates the baseline configuration of the information system as an integral part of information system component installations.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records.

CM-2(CMS-1) – Enhancement (Moderate)

Control

Review and, if necessary, update the baseline configuration and any other system-related operations or security documentation at least once every year, and while planning major system changes / upgrades.

Applicability: All	**References:** ARS: CM-2(CMS-1); FISCAM: TSS-3.2.6	**Related Controls:**

ASSESSMENT PROCEDURE: CM-2(CMS-1).1

Assessment Objective

Determine if the organization develops, documents, and maintains a baseline configuration of the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records to determine the baseline configuration and any other system-related operations or security documentation are reviewed and updated at least once every year, and while planning major system changes / upgrades.
Interview: Organizational personnel with configuration management responsibilities to determine the baseline configuration and any other system-related operations or security documentation are reviewed and updated at least once every year, and while planning major system changes / upgrades.

CM-2(CMS-2) – Enhancement (Moderate)

Control

Maintain an updated list of the information system's operations and security documentation.

Applicability: All	**References:** ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6	**Related Controls:**

ASSESSMENT PROCEDURE: CM-2(CMS-2).1

Assessment Objective

Determine if the organization updates the baseline configuration of the information system as an integral part of information system component installations.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records to determine an updated list of the information system's operations and security documentation is maintained.
Interview: Organizational personnel with configuration management responsibilities to determine an updated list of the information system's operations and security documentation is maintained.

CM-3 – Configuration Change Control (Moderate)

Control

Change control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to control changes to the information system. Change request forms shall be used to document requests with related approvals. Change requests shall be approved by the Business Owner, or his/her designated representative, and other appropriate organization officials including, but not limited to, the system maintainer and information system support staff.

Test plans shall be developed and approved for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control) and shall include appropriate consideration of security. Test results shall be documented and appropriate responsive actions shall be taken based on the results.

Emergency changes for the CMS information system shall be documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration shall be documented appropriately and approved, and responsible personnel shall be notified for security analysis and follow-up.

Guidance

The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system.

Applicability: All	**References:** ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3	**Related Controls:** CM-4, CM-6, SI-2

ASSESSMENT PROCEDURE: CM-3.1

Assessment Objective

Determine if:
(i) the organization authorizes, documents, and controls changes to the information system;
(ii) the organization manages configuration changes to the information system using an organizationally approved process;
(iii) the organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws; and
(iv) the organization audits activities associated with configuration changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system configuration change control; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

CM-3(FIS-1) – Enhancement (Moderate)

Control

Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.

Applicability: All	**References:** FISCAM: TCC-2.1.11	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-1).1

Assessment Objective

Determine if the organization reviews production program changes for access and change control compliance.

Assessment Methods And Objects

Examine: Documentation of management or security administrator reviews.
Examine: Pertinent policies and procedures.
Interview: Information system management or security administrators.

CM-3(FIS-2) – Enhancement (Moderate)

Control

Migration of tested and approved system software to production use is performed by an independent library control group.

Applicability: All	**References:** FISCAM: TSS-3.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-2).1

Assessment Objective

Determine if the organizational independent library control group migrates tested and approved software into production.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation for some system software migrations.

Interview: Management, systems programmers, and library control personnel, and determine who migrates approved system software to production libraries.

CM-3(FIS-3) – Enhancement (Moderate)

Control

Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.

Applicability: All	**References:** FISCAM: TSS-3.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-3).1

Assessment Objective

Determine if the organization provides advance schedules to system users which minimize system software installation impacts.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Recent installations and determine whether scheduling and advance notification did occur.

Interview: Management and systems programmers about scheduling and giving advance notices when system software is installed.

CM-3(FIS-4) – Enhancement (Moderate)

Control

Outdated versions of system software are removed from production libraries.

Applicability: All	**References:** FISCAM: TSS-3.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-4).1

Assessment Objective

Determine if the organization removes outdated versions of system software from the production libraries.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation for the removal of outdated versions from production libraries.

Interview: Management, systems programmers, and library control personnel, and determine whether outdated versions are removed from production libraries.

CM-4 – Monitoring Configuration Changes (Moderate)

Control

Mechanisms to monitor change activity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to monitor information system changes and actions by privileged users. Security impact analyses shall be conducted after system changes are made to determine the IS-related effects of the changes. Activities associated with configuration changes to the information system shall be audited.

Guidance

Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system.

Applicability: All	**References:** ARS: CM-4; FISCAM: TCC-2.1.11, TCC-2.2.2, TCC-2.3.1, TCC-3.1, TSS-3.1.4; NIST 800-53/53A: CM-4; PISP: 4.5.4	**Related Controls:** CA-7, CM-3

ASSESSMENT PROCEDURE: CM-4.1

Assessment Objective

Determine if:

(i) the organization identifies the types of information system changes to be monitored;

(ii) the organization monitors changes to the information system; and

(iii) the organization conducts security impact analyses to assess the effects of the information system changes.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

CM-4(CMS-1) – Enhancement (Moderate)		
Control When changes to the system occur, record the installation of information system components in the appropriate system documentation resource(s).		
Applicability: All	**References:** ARS: CM-4(CMS-1); FISCAM: TCC-2.1.10, TCC-2.2.2, TCC-2.3.1, TCC-3.1, TSS-3.1.4	**Related Controls:**
ASSESSMENT PROCEDURE: CM-4(CMS-1).1		
Assessment Objective Determine if: (i) the organization identifies the types of information system changes to be monitored; (ii) the organization monitors changes to the information system; and (iii) the organization conducts security impact analyses to assess the effects of the information system changes. **Assessment Methods And Objects** **Examine:** Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records to determine that when changes to the system occur, the installation of information system components is recorded in the appropriate system documentation resource(s). **Interview:** Organizational personnel with information system monitoring responsibilities to determine that when changes to the system occur, the installation of information system components is recorded in the appropriate system documentation resource(s).		
CM-4(FIS-1) – Enhancement (Moderate)		
Control Library management software is used to: (1) maintain program version numbers, (2) maintain creation/date information for production modules, (3) maintain copies of previous versions, and (4) control concurrent updates.		
Applicability: All	**References:** FISCAM: TCC-3.1	**Related Controls:**
ASSESSMENT PROCEDURE: CM-4(FIS-1).1		
Assessment Objective Determine if the organization uses library management software to: (1) maintain program version numbers, (2) maintain creation/date information for production modules, (3) maintain copies of previous versions, and (4) control concurrent updates. **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Selection of programs maintained in the library and assess compliance with prescribed procedures. **Interview:** Personnel responsible for library control. **Test:** Verify how many prior versions of software modules are maintained.		
CM-4(FIS-2) – Enhancement (Moderate)		
Control Before and after images of program code are maintained and compared to ensure that only approved changes are made.		
Applicability: All	**References:** FISCAM: TCC-3.3.2	**Related Controls:**
ASSESSMENT PROCEDURE: CM-4(FIS-2).1		
Assessment Objective Determine if the organization ensures only approved program changes are made by maintaining and comparing before and after program code images. **Assessment Methods And Objects** **Examine:** For a selection of program changes, examine related documentation to verify that before and after images were compared. **Examine:** Pertinent policies and procedures. **Interview:** Application programmers, if available.		
CM-5 – Access Restrictions for Change (Moderate)		
Control Access control change mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to approve individual access privileges and to enforce physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.		

Guidance

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

Applicability: All	**References:** ARS: CM-5; FISCAM: TCC-3.2.3, TCC-3.3.1, TSS-1.2.1, TSS-1.2.2, TSS-3.1.4, TSS-3.2.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-5; PISP: 4.5.5	**Related Controls:**

ASSESSMENT PROCEDURE: CM-5.1

Assessment Objective

Determine if:
(i) the organization maintains a list of qualified and authorized personnel permitted to access the information system for the express purpose of initiating changes;
(ii) the organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and
(iii) the organization generates, retains, and reviews records reflecting all such changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.
Test: Change control process and associated restrictions for changes to the information system.(Optional)

CM-6 – Configuration Settings (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to configure and benchmark information technology products in accordance with good security practice settings. Mandatory configuration settings for information technology products employed within the information system shall be established. The security settings of information technology products shall be configured to the most restrictive mode consistent with information system operational requirements, documented, and enforced in all components of the information system.

Guidance

Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems.

Applicability: All	**References:** ARS: CM-6; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6; PISP: 4.5.6	**Related Controls:** CM-2, CM-3, CM-8, SI-4

ASSESSMENT PROCEDURE: CM-6.1

Assessment Objective

Determine if:
(i) the organization establishes mandatory configuration settings for information technology products employed within the information system;
(ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;
(iii) the organization documents the configuration settings; and
(iv) the organization enforces the configuration settings in all components of the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST SP 800-70; other relevant documents or records.
Test: Information system configuration settings.

CM-6(CMS-1) – Enhancement (Moderate)

Control

Configure the information system to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

Applicability: All	**References:** ARS: CM-6(CMS-1); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-6(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes mandatory configuration settings for information technology products employed within the information system;
(ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; and
(iii) the organization documents the configuration settings.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST SP 800-70; other relevant documents or records to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

Interview: Organizational personnel with configuration management responsibilities to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

Test: Information system to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

CM-7 – Least Functionality (Moderate)

Control

Information systems shall be configured to provide only essential capabilities. The functions and services provided by CMS information systems shall be reviewed carefully to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol [VoIP], Instant Messaging [IM], File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP], file sharing). The use of those functions, ports, protocols, and/or services shall be prohibited and/or restricted.

Guidance

Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Applicability: All	**References:** ARS: CM-7; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7; PISP: 4.5.7	**Related Controls:**

ASSESSMENT PROCEDURE: CM-7.1

Assessment Objective

Determine if:

(i) the organization identifies prohibited or restricted functions, ports, protocols, and services for the information system;

(ii) the organization configures the information system to provide only essential capabilities; and

(iii) the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for disabling or restriction of functions, ports, protocols, and services.

CM-7(0) – Enhancement (Moderate)

Control

Configure the information system specifically to only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system / application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.

Applicability: All	**References:** ARS: CM-7(0); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7; PISP: 4.5.7	**Related Controls:**

ASSESSMENT PROCEDURE: CM-7(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan (for list of organization-defined prohibited or restricted functions, ports, protocols, and services for the information system); information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system configuration settings.

CM-8 – Information System Component Inventory (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to document and maintain a current inventory of the information system's constituent components and relevant ownership information. The inventory of information system components shall include manufacturer, model / type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership.

Guidance

The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system.

Applicability: All	**References:** ARS: CM-8; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8; PISP: 4.5.8	**Related Controls:** CM-2, CM-6

ASSESSMENT PROCEDURE: CM-8.1

Assessment Objective

Determine if:
(i) the organization develops, documents, and maintains a current inventory of the components of the information system; and
(ii) the inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system inventory records; other relevant documents or records.

CM-8(1) – Enhancement (Moderate)

Control

Update the information system component inventory as an integral part of component installations.

Applicability: All	**References:** ARS: CM-8(1); HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CM-8(1).1

Assessment Objective

Determine if the organization updates the inventory of information system components as an integral part of component installations.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records.

Interview: Organizational personnel with information system installation and inventory responsibilities.(Optional)

Contingency Planning (CP) – *Operational*

CP-1 – Contingency Planning Policy and Procedures (Moderate)

Control

All major CMS information systems shall be covered by a CP that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

Guidance

The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-34 provides guidance on contingency planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CP-1; FISCAM: TSC-2.2.2; HIPAA: 164.308(a)(7)(i), 164.308(a)(7)(ii)(B); IRS-1075: 5.6.2.2#1.1; NIST 800-53/53A: CP-1; PISP: 4.6.1	**Related Controls:**

ASSESSMENT PROCEDURE: CP-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents contingency planning policy and procedures;
(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and
(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: CP-1.2

Assessment Objective

Determine if:
(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

CP-2 – Contingency Plan (Moderate)

Control

All major CMS information systems shall be covered by a CP, relative to the system security level, providing continuity of support in the event of a disruption of service. A CP for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A CP for the information system shall be consistent with NIST SP 800-34. Designated officials within the organization shall review and approve the CP and distribute copies of the plan to key contingency personnel.

Guidance

Contingency Plans consist of all components listed in the CMS Business Partners system Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.

Applicability: All	**References:** ARS: CP-2; FISCAM: TSC-1.1, TSC-1.2, TSC-1.3, TSC-2.1.2, TSC-3.1.1, TSC-3.1.2, TSC-3.1.3, TSC-3.1.4, TSC-3.2.3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.3; NIST 800-53/53A: CP-2; PISP: 4.6.2	**Related Controls:**

ASSESSMENT PROCEDURE: CP-2.1

Assessment Objective

Determine if:

(i) the organization develops and documents a contingency plan for the information system;
(ii) the contingency plan is consistent with NIST SP 800-34;
(iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure;
(iv) the contingency plan is reviewed and approved by designated organizational officials; and
(v) the organization disseminates the contingency plan to key contingency personnel.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; NIST SP 800-34; contingency plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-2.2

Assessment Objective

Determine if key contingency personnel and the key operating elements within the organization understand the contingency plan and are ready to implement the plan.

Assessment Methods And Objects

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-2(1) – Enhancement (Moderate)

Control

Coordinate development of the Contingency Plan (CP) with parties responsible for related plans, such as the Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan (COOP), Business Recovery Plan, and Incident Response Plan.

Guidance

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

Applicability: All	**References:** ARS: CP-2(1); FISCAM: TSC-3.1.3; HIPAA: 164.308(a)(7)(ii)(E); HSPD 7: G(22)(i); NIST 800-53/53A: CP-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-2(1).1

Assessment Objective

Determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas.

CP-2(2) – Enhancement (Moderate)

Control

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

Applicability: All	**References:** ARS: CP-2(2); HSPD 7: G(22)(i)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-2(2).1

Assessment Objective

Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records.(Optional)
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

CP-3 – Contingency Training (Moderate)

Control

Operational and support personnel (including managers and users of the information system) shall receive training in contingency operations and understand their contingency roles and responsibilities with respect to the information system. Refresher training shall be provided to all contingency personnel.

Guidance

Managers, responsible for contingency operations, and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirmed that appropriate training has been completed.

Applicability: All	References: ARS: CP-3; FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3	Related Controls:

ASSESSMENT PROCEDURE: CP-3.1

Assessment Objective

Determine if:
(i) the organization provides contingency training to personnel with significant contingency roles and responsibilities;
(ii) the organization records the type of contingency training received and the date completed;
(iii) the organization defines frequency of refresher contingency training; and
(iv) the organization provides initial training and refresher training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan; other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

ASSESSMENT PROCEDURE: CP-3.2

Assessment Objective

Determine if contingency training material addresses the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.

CP-3(0) – Enhancement (Moderate)

Control

Provide training every 365 days in contingency roles and responsibilities.

Applicability: All	References: ARS: CP-3(0); FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3	Related Controls:

ASSESSMENT PROCEDURE: CP-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan (for organization-defined frequency for refresher contingency training); other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-4 – Contingency Plan Testing and Exercises (Moderate)

Control

CPs shall be tested and/or exercised at least every 365 days using defined tests and exercises, such as the tabletop test in accordance with current CMS Procedures, to determine the plans' effectiveness and readiness to execute the plan. Test / exercise results shall be documented and reviewed by appropriate organization officials. Reasonable and appropriate corrective actions shall be initiated to close or reduce the impact of CP failures and deficiencies.

Guidance

There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Applicability: All	References: ARS: CP-4; FISCAM: TSC-1.1, TSC-4.1, TSC-4.2.1, TSC-4.2.2; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2; NIST 800-53/53A: CP-4; PISP: 4.6.4	Related Controls:

ASSESSMENT PROCEDURE: CP-4.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of contingency plan tests and/or exercises;

(ii) the organization defines the set of contingency plan tests and/or exercises;
(iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;
(iv) the organization documents the results of contingency plan testing/exercises; and
(v) the organization reviews the contingency plan test/exercise results and takes corrective actions.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-4.2

Assessment Objective

Determine if the contingency plan tests/exercises address key aspects of the plan.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records.

CP-4(0) – Enhancement (Moderate)

Control

The CP must be current and executable, tested using a combination of tabletop exercises and operational tests every 365 days, and updated as needed.

Applicability: All	**References:** ARS: CP-4(0); FISCAM: TSC-4.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-4; PISP: 4.6.4	**Related Controls:**

ASSESSMENT PROCEDURE: CP-4(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan (for the organization-defined frequency of contingency plan tests and/or exercises and the list of the organization-defined contingency plan tests and/or exercises); contingency plan testing and/or exercise documentation; other relevant documents or records.

CP-4(1) – Enhancement (Moderate)

Control

Coordinate testing and exercising of CP with parties responsible for related plans, such as:
(a) Business Continuity Plan,
(b) Disaster Recovery Plan,
(c) Continuity of Operations Plan,
(d) Business Recovery Plan, and
(e) Incident Response Plan.

Guidance

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

Applicability: All	**References:** ARS: CP-4(1); HSPD 7: G(22)(i); NIST 800-53/53A: CP-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-4(1).1

Assessment Objective

Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities.

CP-5 – Contingency Plan Update (Moderate)

Control

CPs shall be reviewed at least every 365 days and, if necessary, revised to address system / organizational changes and/or any problems encountered during plan implementation, execution, or

testing.

Guidance

Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Applicability: All	**References:** ARS: CP-5; FISCAM: TSC-1.1, TSC-3.1.5; HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	**Related Controls:**

ASSESSMENT PROCEDURE: CP-5.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of contingency plan reviews and updates;
(ii) the organization updates the contingency plan in accordance with organization-defined frequency, at least annually; and
(iii) the revised plan addresses the system/organizational changes identified by the organization or any problems encountered by the organization during plan implementation, execution, and testing.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-5.2

Assessment Objective

Determine if the organization communicates necessary changes to the contingency plan to other organizational elements with related plans.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records.
Interview: Organizational personnel with contingency plan update responsibilities; organizational personnel with mission-related and operational responsibilities.

CP-5(0) – Enhancement (Moderate)

Control

Review the CP at least every 365 days and update, as necessary, to address: system, organizational, or facility changes; problems encountered during plan implementation, execution, or testing; or other conditions that may impact the system CP.

Applicability: All	**References:** ARS: CP-5(0); HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	**Related Controls:**

ASSESSMENT PROCEDURE: CP-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan (for organization-defined frequency of contingency plan reviews and updates); other relevant documents or records.
Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records.
Interview: Organizational personnel with contingency plan review and update responsibilities; organizational personnel with mission-related and operational responsibilities.

CP-6 – Alternate Storage Site (Moderate)

Control

Agreements with an alternate storage site shall be established and implemented effectively to permit the storage of CMS information system backup information. Copies of the current CP shall be stored in a secure location at an alternate site accessible by management and other key personnel. Procedures shall be developed, documented, and implemented effectively to respond to contingencies by ensuring separation of routine information system operations and the alternate storage site.

Guidance

The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Applicability: All	**References:** ARS: CP-6; IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6; PISP: 4.6.6	**Related Controls:**

ASSESSMENT PROCEDURE: CP-6.1

Assessment Objective

Determine if:
(i) the organization identifies an alternate storage site; and

(ii) alternate storage site agreements are currently in place (if needed) to permit storage of information system backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-6.2

Assessment Objective

Determine if the alternate storage site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information consistent with the organization's recovery time objectives and recovery point objectives.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

Interview: Organizational personnel with alternate storage site responsibilities.(Optional)

CP-6(1) – Enhancement (Moderate)

Control

Ensure that the alternate storage site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.

Applicability: All	**References:** ARS: CP-6(1); FISCAM: TSC-2.1.3; IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-6(1).1

Assessment Objective

Determine if:

(i) the contingency plan identifies the primary storage site hazards; and

(ii) the alternate storage site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

CP-6(3) – Enhancement (Moderate)

Control

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and document explicit mitigation actions.

Applicability: All	**References:** ARS: CP-6(3); IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(3)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-6(3).1

Assessment Objective

Determine if:

(i) the contingency plan identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and

(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

CP-7 – Alternate Processing Site (Moderate)

Control

Agreements with an alternate processing site shall be established and implemented to permit the resumption of CMS information system operations for mission critical business functions when the primary processing capabilities are unavailable, and the CP calls for application recovery in place of other accepted processes. Procedures shall be developed, documented, and implemented effectively to establish contingency activities and responsibilities.

Guidance

Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives.

Applicability: All	**References:** ARS: CP-7; FISCAM: TSC-3.2.1; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7; PISP: 4.6.7	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7.1

Assessment Objective

Determine if:

(i) the organization identifies an alternate processing site;

(ii) the organization defines the time period within which processing must be resumed at the alternate processing site; and
(iii) alternate processing site agreements are currently in place (if needed) to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-7.2

Assessment Objective

Determine if the alternate processing site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.
Interview: Organizational personnel with alternate processing site responsibilities.(Optional)

CP-7(0) – Enhancement (Moderate)

Control

Ensure all equipment and supplies required for resuming information system operations for critical functions within seventy-two (72) hours after COOP activation are available at the alternate processing site, or contracts are in place to support delivery to the site.

Applicability: All	**References:** ARS: CP-7(0); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7; PISP: 4.6.7	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan (for organization-defined time period within which processing must be resumed at the alternate processing site); other relevant documents or records.
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.
Interview: Organizational personnel with alternate processing site responsibilities.(Optional)

CP-7(1) – Enhancement (Moderate)

Control

Ensure the alternate processing site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.

Applicability: All	**References:** ARS: CP-7(1); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(1).1

Assessment Objective

Determine if:
(i) the contingency plan identifies the primary processing site hazards; and
(ii) the alternate processing site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

CP-7(2) – Enhancement (Moderate)

Control

Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Applicability: All	**References:** ARS: CP-7(2); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(2).1

Assessment Objective

Determine if:
(i) the contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and
(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

CP-7(3) – Enhancement (Moderate)

Control

Ensure alternate processing site agreements contain appropriate priority-of-service provisions.

Applicability: All	**References:** ARS: CP-7(3); FISCAM: TSC-3.2.1; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(3)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-7(3).1

Assessment Objective

Determine if alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records.

CP-8 – Telecommunications Services (Moderate)

Control

Necessary agreements shall be established and implemented for alternate communications services capable of restoring adequate communications to accomplish mission critical functions when the primary operations and communications capabilities are unavailable.

Guidance

In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).

Applicability: All	**References:** ARS: CP-8; FISCAM: TSC-3.2.2; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8; PISP: 4.6.8	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8.1

Assessment Objective

Determine if:
(i) the organization identifies primary and alternate telecommunications services to support the information system;
(ii) the organization defines the time period within which resumption of information system operations must take place; and
(iii) alternate telecommunications service agreements are in place to permit the resumption of telecommunications services for critical mission/business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; information system security plan; primary and alternate telecommunications service agreements; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-8.2

Assessment Objective

Determine if:
(i) telecommunications services supporting the organization are used for national security emergency preparedness; and
(ii) a common carrier provides telecommunications services.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

CP-8(0) – Enhancement (Moderate)

Control

Resume system operations for critical functions within seventy-two (72) hours when the primary telecommunications capabilities are unavailable.

Applicability: All	**References:** ARS: CP-8(0); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8; PISP: 4.6.8	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; information system security plan (for organization-defined time period within which resumption of information system operations must take place); primary and alternate telecommunications service agreements; other relevant documents or records.

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

CP-8(1) – Enhancement (Moderate)

Control

Ensure agreements with primary and alternate telecommunication service providers include priority-of-service provisions.

Applicability: All	**References:** ARS: CP-8(1); FISCAM: TSC-3.2.2; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8(1).1

Assessment Objective

Determine if primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the availability requirements defined in the organization's contingency plan.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

CP-8(2) – Enhancement (Moderate)

Control

Ensure alternate telecommunication providers do not share a single point of failure with primary telecommunications services.

Applicability: All	**References:** ARS: CP-8(2); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(2)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-8(2).1

Assessment Objective

Determine if primary and alternate telecommunications services share a single point of failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

CP-9 – Information System Backup (Moderate)

Control

Backup mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable the backing-up of user-level and system-level information (including system state information) contained in the CMS information system. The frequency of information system backups and the transfer rate of backup information to an alternate storage site (if so designated) shall be consistent with the CMS recovery time objectives and recovery point objectives.

Mechanisms shall provide for sufficient backup storage capability. Checkpoint capabilities shall be part of any backup operation that updates files and consumes large amounts of information system time. Backup copies of CMS data shall be created on a regular basis, and appropriate safeguards shall be implemented to protect the technical and physical security of backup media at the storage location. Where appropriate, backup copies of all other forms of data, including paper records, shall be created based upon an assessment of the level of data criticality and the corresponding risk of data loss.

Guidance

The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time. The protection of system backup information while in transit is beyond the scope of this control.

Applicability: All	**References:** ARS: CP-9; FISCAM: TSC-2.1.1, TSC-2.1.3; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	**Related Controls:** MA-CMS-1, MA-CMS-2, MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of information systems backups;
(ii) the organization defines the user-level and system-level information (including system state information) that is required to be backed up; and
(iii) the organization identifies the location(s) for storing backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records.

ASSESSMENT PROCEDURE: CP-9.2

Assessment Objective

Determine if:
(i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency;
(ii) the organization stores backup information in designated locations in accordance with information system backup procedures; and
(iii) the organization protects backup information at the designated storage locations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records.

CP-9(0) – Enhancement (Moderate)

Control

Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time and action.

Applicability: All	**References:** ARS: CP-9(0); HIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	**Related Controls:**

ASSESSMENT PROCEDURE: CP-9(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for information system backup); backup storage location(s); other relevant documents or records.

CP-9(1) – Enhancement (Moderate)

Control

Test backup information to verify media reliability and information integrity, following each backup.

Applicability: All	**References:** ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-9(1).1

Assessment Objective

Determine if:
(i) the organization defines the frequency of information system backup testing;
(ii) the organization conducts information system backup testing within the organization-defined frequency; and
(iii) testing results verify backup media reliability and information integrity.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; information system backup test results; backup storage location(s); other relevant documents or records.

CP-9(4) – Enhancement (Moderate)

Control

Protect backup information from unauthorized modification.

Guidance

The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control.

Applicability: All	**References:** ARS: CP-9(4); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(4)	**Related Controls:** MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9(4).1

Assessment Objective

Determine if the organization employs appropriate mechanisms to protect the integrity of information system backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; backup storage location(s); information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with information system backup responsibilities.

CP-9(PII-1) – Enhancement (Moderate)

Control

Insure that a current, retrievable, copy of PII is available before movement of servers.

Applicability: All	**References:** HIPAA: 164.310(d)(2)(iv)	**Related Controls:**

ASSESSMENT PROCEDURE: CP-9(PII-1).1

Assessment Objective

Determine if the organization ensures a current and retrievable copy of PII is available before movement of servers.

Assessment Methods And Objects

Examine: EPHI Server Movement Plan is addresses in the COOP and backup procedures are available. A current copy of PII is available.

Interview: Organizational personnel with PII backup responsibilities to determine if the PII copy is current and retrievable.

Test: Following the data backup and reconstitution procedures for PII, determine if the current copy is retrievable.

CP-10 – Information System Recovery and Reconstitution (Moderate)

Control

Information system recovery and reconstitution mechanisms with supporting procedures shall be developed, documented, and implemented effectively to allow the CMS information system to be recovered and reconstituted to a known secure state after a disruption or failure. Recovery of CMS information systems after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

Guidance

Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Applicability: All	**References:** ARS: CP-10; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10; PISP: 4.6.10	**Related Controls:**

ASSESSMENT PROCEDURE: CP-10.1

Assessment Objective

Determine if the organization identifies the means for capturing the information system's operational state including appropriate system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-10.2

Assessment Objective

Determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

Test: Automated mechanisms implementing information system recovery and reconstitution operations.

CP-10(0) – Enhancement (Moderate)		
Control Secure information system recovery and reconstitution includes, but not limited to: (a) Reset all system parameters (either default or organization-established), (b) Reinstall patches, (c) Reestablish configuration settings, (d) Reinstall application and system software, and (e) Fully test the system.		
Applicability: All	**References:** ARS: CP-10(0); NIST 800-53/53A: CP-10; PISP: 4.6.10	**Related Controls:**
ASSESSMENT PROCEDURE: CP-10(0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test:** Automated mechanisms implementing information system recovery and reconstitution operations.		

Identification and Authentication (IA) – *Technical*

IA-1 – Identification and Authentication Policy and Procedures (Moderate)

Control

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

Guidance

The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and SP 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**References:** ARS: IA-1; IRS-1075: 5.6.3.1#1.1; NIST 800-53/53A: IA-1; PISP: 4.7.1	**Related Controls:**

ASSESSMENT PROCEDURE: IA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents identification and authentication policy and procedures;
(ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review identification and authentication policy and procedures; and
(iv) the organization updates identification and authentication policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.
Interview: Organizational personnel with identification and authentication responsibilities.(Optional)

ASSESSMENT PROCEDURE: IA-1.2

Assessment Objective

Determine if:
(i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.
Interview: Organizational personnel with identification and authentication responsibilities.(Optional)

IA-2 – User Identification and Authentication (Moderate)

Control

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique IA of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

Guidance

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in SP 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST SP 800-63 level 1 compliant. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST SP 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals.

Applicability: All	**References:** ARS: IA-2; FISCAM: TAC-3.2.A.4, TAN-2.1.4; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 5.6.3.1#1.2, 5.6.3.3#2.3; NIST 800-53/53A: IA-2; PISP: 4.7.2	**Related Controls:** AC-14, AC-17, MA-4

ASSESSMENT PROCEDURE: IA-2.1

Assessment Objective

Determine if:
(i) the information system uniquely identifies and authenticates users (or processes acting on behalf of users); and
(ii) authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63 and e-authentication risk assessment results.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; e-authentication risk assessment results; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(1) – Enhancement (Moderate)

Control

Employ multifactor authentication for remote system access that is at least NIST SP 800-63 level 3 compliant.

Applicability: All	**References:** ARS: IA-2(1); FISCAM: TAN-2.1.7; HIPAA: 164.312(d); IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: IA-2(1).1

Assessment Objective

Determine if:
(i) the organization defines the NIST SP 800-63 authentication levels for the information system; and
(ii) the information system employs multifactor authentication for remote system access that is NIST SP 800-63 compliant in accordance with the organizational selection of level 3, level 3 using a hardware authentication device, or level 4.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-2(CMS-1) – Enhancement (Moderate)

Control

Require the use of unique user identifiers and system and/or network authenticators.

Applicability: All	**References:** ARS: IA-2(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4, TAN-2.1.4, TAN-2.1.7; IRS-1075: 5.6.3.1#1.2	**Related Controls:**

ASSESSMENT PROCEDURE: IA-2(CMS-1).1

Assessment Objective

Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine the use of unique user identifiers and system and/or network authenticators is required.
Interview: Organizational personnel with identification and authentication responsibilities to determine the use of unique user identifiers and system and/or network authenticators is required.
Test: Automated mechanisms implementing identification and authentication capability for the information system to determine the use of unique user identifiers and system and/or network authenticators is required.

IA-2(CMS-2) – Enhancement (Moderate)

Control

All passwords shall be encrypted in transit and at rest.

Applicability: All	References: ARS: IA-2(CMS-2); FISCAM: TAC-3.2.A.1, TAC-3.2.A.7; IRS-1075: 5.6.3.1#1.2	Related Controls:

ASSESSMENT PROCEDURE: IA-2(CMS-2).1

Assessment Objective

Determine if authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine all passwords are required to be encrypted in transit and at rest.

Interview: Organizational personnel with identification and authentication responsibilities to determine to determine all passwords are required to be encrypted in transit and at rest.

Test: Automated mechanisms implementing identification and authentication capability for the information system to determine all passwords are required to be encrypted in transit and at rest.

IA-2(CMS-3) – Enhancement (Moderate)

Control

Help desk support requires user identification for any transaction that has information security implications.

Applicability: All	References: ARS: IA-2(CMS-3)	Related Controls:

ASSESSMENT PROCEDURE: IA-2(CMS-3).1

Assessment Objective

Determine if authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine help desk support requires user identification for any transaction that has information security implications.

Interview: Organizational personnel with identification and authentication responsibilities to determine to determine help desk support requires user identification for any transaction that has information security implications.

Test: Automated mechanisms implementing identification and authentication capability for the information system to determine help desk support requires user identification for any transaction that has information security implications.

IA-3 – Device Identification and Authentication (Moderate)

Control

Automated mechanisms shall be used to enable IA of the CMS information system being used and to which a connection is being made before establishing a connection.

Guidance

The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802. 1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Applicability: All	References: ARS: IA-3; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	Related Controls:

ASSESSMENT PROCEDURE: IA-3.1

Assessment Objective

Determine if:

(i) the organization defines specific devices requiring identification and authentication before establishing connections to the information system; and

(ii) the information system identifies and authenticates specific devices identified by the organization before establishing connections.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing device identification and authentication.(Optional)

IA-3(0) – Enhancement (Moderate)

Control

Implement an information system that uses either a shared secret or digital certificate to identify and authenticate specific devices before establishing a connection.

Applicability: All	References: ARS: IA-3(0); IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	Related Controls:

ASSESSMENT PROCEDURE: IA-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; information system design documentation; procedures addressing device identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing device identification and authentication.(Optional)

IA-4 – Identifier Management (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to manage user identifiers. The procedures shall address processes and controls for:

4.7.4.1. Identifying each user uniquely;
4.7.4.2. Verifying the identity of each user;
4.7.4.3. Receiving authorization to issue a user identifier from an appropriate organization official;
4.7.4.4. Ensuring that the user identifier is issued to the intended party;
4.7.4.5. Disabling user identifier after a specific period of inactivity; and
4.7.4.6. Archiving user identifiers.

Reviews and validation of system users' accounts shall be conducted to ensure the continued need for access to a system. Identifier management shall not be applicable to shared information system accounts (i.e., guest and anonymous).

Guidance

Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors.

Applicability: All	**References:** ARS: IA-4; FISCAM: TAC-3.2.A.4, TAN-2.1.4; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-4; PISP: 4.7.4	**Related Controls:**

ASSESSMENT PROCEDURE: IA-4.1

Assessment Objective

Determine if:

(i) the organization manages user identifiers by uniquely identifying each user;
(ii) the organization manages user identifiers by verifying the identity of each user;
(iii) the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official;
(iv) the organization manages user identifiers by issuing the identifier to the intended party;
(v) the organization defines the time period of inactivity after which a user identifier is to be disabled;
(vi) the organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and
(vii) the organization manages user identifiers by archiving identifiers.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

Test: Identity verification capability for the information system and for organizational facilities.

ASSESSMENT PROCEDURE: IA-4.2

Assessment Objective

Determine if the organization uses a Personal Identity Verification (PIV) card token to uniquely identify and authenticate federal employees and contractors in accordance with FIPS 201 and NIST SP 800-73, 800-76, and 800-78.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST SP 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

Test: Identity verification capability for the information system and for organizational facilities.

IA-4(0) – Enhancement (Moderate)		
Control Disable user identifiers after 180 days of inactivity and delete disabled accounts during annual re-certification process.		
Applicability: All	**References:** ARS: IA-4(0); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.1#2, 5.6.3.2#2.1; NIST 800-53/53A: IA-4; PISP: 4.7.4	**Related Controls:** AC-2(3)
ASSESSMENT PROCEDURE: IA-4(0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. **Test:** Identity verification capability for the information system and for organizational facilities. **Examine:** Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST SP 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.		
IA-4(CMS-1) – Enhancement (Moderate)		
Control Require system administrator to maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.		
Applicability: All	**References:** ARS: IA-4(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4; IRS-1075: 5.6.3.1#2	**Related Controls:** AC-2(CMS-2)
ASSESSMENT PROCEDURE: IA-4(CMS-1).1		
Assessment Objective Determine if the organization manages user identifiers by uniquely identifying each user. **Assessment Methods And Objects** **Examine:** Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities. **Interview:** Organizational personnel with identification and authentication responsibilities to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities. **Test:** Identity verification capability for the information system and for organizational facilities to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.		
IA-4(CMS-2) – Enhancement (Moderate)		
Control For non-CMS entities to issue user identifiers, receive prior written approval from the CIO or his/her designated representative.		
Applicability: All	**References:** ARS: IA-4(CMS-2)	**Related Controls:**
ASSESSMENT PROCEDURE: IA-4(CMS-2).1		
Assessment Objective Determine if responsible parties within the organization periodically review identification and authentication policy and procedures. **Assessment Methods And Objects** **Examine:** Identification and authentication policy and procedures; other relevant documents or records to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers. **Interview:** Organizational personnel with identification and authentication management responsibilities to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers.		
IA-4(FIS-1) – Enhancement (Moderate)		
Control Personnel files are matched with actual system users to remove terminated or transferred employees from the system.		
Applicability: All	**References:** FISCAM: TAC-3.2.A.6	**Related Controls:**

ASSESSMENT PROCEDURE: IA-4(FIS-1).1

Assessment Objective

Determine if the organizational personnel files are automatically [or manually] matched with actual system users to remove terminated or transferred employees from the system.

Assessment Methods And Objects

Examine: Documentation of such comparisons.
Examine: Pertinent policies and procedures.
Interview: Security managers.

IA-5 – Authenticator Management (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to manage user authenticators. The procedures shall address processes and controls for: initial authenticator content; distribution for new, lost, compromised, or damaged authenticators; revocation of authenticators; changing default authenticators; and changing / refreshing authenticators at specified intervals. Users shall not loan or share authenticators with other users. Lost or compromised authenticators shall be reported immediately to appropriate authority.

Selection of passwords or other authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS System Security Level of the information system. Automated mechanisms shall be in place for password-based authentication, to ensure that the information system:
4.7.5.1. Protects passwords from unauthorized disclosure and modification when stored and transmitted;
4.7.5.2. Prohibits passwords from being displayed when entered;
4.7.5.3. Enforces automatic expiration of passwords;
4.7.5.4. Prohibits password reuse for a specified number of generations; and
4.7.5.5. Enforces periodic password changes.

Guidance

Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**References:** ARS: IA-5; FISCAM: TAC-3.2.A.1, TAC-3.2.A.3; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	**Related Controls:** AC-11(0), AC-CMS-1(CMS-2)

ASSESSMENT PROCEDURE: IA-5.1

Assessment Objective

Determine if:
(i) the organization manages information system authenticators by defining initial authenticator content;
(ii) the organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;
(iii) the organization manages information system authenticators by changing default authenticators upon information system installation; and
(iv) the organization manages information system authenticators by changing/refreshing authenticators periodically.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Automated mechanisms implementing authenticator management functions.

IA-5(0) – Enhancement (Moderate)

Control

For password-based authentication:
(a) Protect passwords from disclosure or modification when stored or transmitted,
(b) Prevent passwords from being displayed when entered,
(c) When using passwords in connection with e-authentication, refer to ARS Appendix A, e-Authentication Standards for further guidance,

(d) Force users to select a password comprising a minimum of eight (8) alphanumeric and/or special characters,
(e) Automatically force users (including administrators) to change account and system account passwords every sixty (60) days,
(f) Automatically force users to select six (6) unique passwords prior to reusing a previous one, and
(g) Enforce password lifetime restrictions within a minimum of one (1) day and maximum of sixty (60) days.

Applicability: All	**References:** ARS: IA-5(0); HIPAA: 164.308(a)(5)(ii)(D); IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Automated mechanisms implementing authenticator management functions.

IA-5(FIS-1) – Enhancement (Moderate)

Control

For devices such as tokens or key cards, users: (1) maintain possession of their individual tokens, cards, etc., and (2) understand that they must not loan or share these with others, and must report lost items immediately.

Applicability: All	**References:** FISCAM: TAC-3.2.A.8	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(FIS-1).1

Assessment Objective

Determine if:
(i) the organizational users maintain possession of their individual devices such as tokens or key cards, etc.; and
(ii) the organizational users understand they must not loan or share their individual tokens, cards, etc., and report lost items immediately.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Token or key card acknowledgment forms.
Interview: Token and/or key card users.

IA-5(DIR-1) – Enhancement (Moderate)

Control

For password-based authentication, passwords are:
(a) unique for specific individuals, not groups;
(b) controlled by the assigned user and not subject to disclosure;
(c) not displayed when entered;
(d) changed every 60 days, when an individual changes positions, or when security is breached;
(e) at least 8 characters in length;
(f) must include at least one number, one upper and lower case character, and one special character;
(g) prohibited from reuse for at least 6 generations;
(h) prohibited from being changed more than once in a 24-hour period; and
(i) all passwords are encrypted in transit and at rest. The use of dictionary names or words as passwords is prohibited.

Applicability: All	**References:** FISCAM: TAC-3.2.A.1, TAC-3.2.A.2, TAN-2.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(DIR-1).1

Assessment Objective

Determine if the organization effectively uses password and user identification as one tool for security in-depth.

Assessment Methods And Objects

Examine: Password and user identification policy and acceptable user training policy for completeness in meeting the CMS password controls.
Interview: A sampling of users know the organization's policy for password and user system identification.
Test: Using an appropriate system guide or script check the system password configuration:
(a) unique for specific individuals, not groups;

(b) controlled by the assigned user and not subject to disclosure;
(c) not displayed when entered;
(d) changed every 60 days, when an individual changes positions, or when security is breached;
(e) at least 8 characters in length;
(f) must include at least one number, one upper and lower case character, and one special character;
(g) prohibited from reuse for at least 6 generations;
(h) prohibited from being changed more than once in a 24-hour period; and
(i) all passwords are encrypted in transit and at rest. The use of dictionary names or words as passwords is prohibited.

IA-6 – Authenticator Feedback (Moderate)

Control

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to obscure feedback to users during the authentication process to protect the information from possible exploitation / use by unauthorized individuals.

Guidance

The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Applicability: All	**References:** ARS: IA-6; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-6; PISP: 4.7.6	**Related Controls:**

ASSESSMENT PROCEDURE: IA-6.1

Assessment Objective

Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing authenticator feedback.

IA-6(0) – Enhancement (Moderate)

Control

Configure the information system to obscure passwords during the authentication process (e.g., display asterisks).

Applicability: All	**References:** ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6	**Related Controls:**

ASSESSMENT PROCEDURE: IA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing authenticator feedback.

IA-7 – Cryptographic Module Authentication (Moderate)

Control

Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Guidance

The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	**References:** ARS: IA-7; NIST 800-53/53A: IA-7; PISP: 4.7.7	**Related Controls:**

ASSESSMENT PROCEDURE: IA-7.1

Assessment Objective

Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for

authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).

Assessment Methods And Objects

Examine: Identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing cryptographic module authentication.

Incident Response (IR) – *Operational*

IR-1 – Incident Response Policy and Procedures (Moderate)

Control

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed, documented, and implemented effectively to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-61 and current CMS Procedures.

Guidance

The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

Applicability: All	**References:** ARS: IR-1; FISCAM: TSP-3.4; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1; NIST 800-53/53A: IR-1; PISP: 4.8.1	**Related Controls:**

ASSESSMENT PROCEDURE: IR-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents incident response policy and procedures;
(ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review incident response policy and procedures; and
(iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.
Interview: Organizational personnel with incident response planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: IR-1.2

Assessment Objective

Determine if:
(i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.
Interview: Organizational personnel with incident response planning and plan implementation responsibilities.(Optional)

IR-2 – Incident Response Training (Moderate)

Control

All personnel shall be trained in their IR roles and responsibilities with respect to a CMS information system. Personnel shall receive periodic refresher training in IR procedures.

Guidance

Procedures and incident response training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.
(2) Executives must receive training in information security basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.

(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	**References:** ARS: IR-2; IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-2; PISP: 4.8.2	**Related Controls:**

ASSESSMENT PROCEDURE: IR-2.1

Assessment Objective

Determine if:
(i) the organization identifies and documents personnel with incident response roles and responsibilities;
(ii) the organization provides incident response training to personnel with incident response roles and responsibilities;
(iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;
(iv) the organization defines the frequency of refresher incident response training; and
(v) the organization provides refresher incident response training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response training; incident response training material; information system security plan; incident response training records; other relevant documents or records.
Interview: Organizational personnel with incident response training and operational responsibilities.

IR-2(0) – Enhancement (Moderate)

Control

Provide training on incident response roles and responsibilities of personnel every 365 days.

Applicability: All	**References:** ARS: IR-2(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-2; PISP: 4.8.2	**Related Controls:**

ASSESSMENT PROCEDURE: IR-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response training; incident response training material; information system security plan (for organization-defined frequency for refresher incident response training); incident response training records; other relevant documents or records.
Interview: Organizational personnel with incident response training and operational responsibilities.

IR-3 – Incident Response Testing and Exercises (Moderate)

Control

The IR capability for a CMS information system shall be tested periodically using appropriate tests, procedures, automated mechanisms, and exercises to determine the plan's effectiveness. The test results, procedures, and exercises employed to conduct the test shall be documented.

Guidance

NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Applicability: All	**References:** ARS: IR-3; IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-3.1

Assessment Objective

Determine if:
(i) the organization defines incident response tests/exercises;
(ii) the organization defines the frequency of incident response tests/exercises;
(iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency; and
(iv) the organization documents the results of incident response tests/exercises.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan; incident response testing material; incident response test results; other relevant documents or records.

IR-3(0) – Enhancement (Moderate)		
Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations.		
Applicability: All	**References:** ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3	**Related Controls:**
ASSESSMENT PROCEDURE: IR-3(0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of organization-defined tests/exercises and organization-defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant documents or records.		
IR-4 – Incident Handling (Moderate)		
Control An incident handling capability, which includes preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents, shall be established and maintained. Evidence of computer crimes, computer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learned from on-going incident handling activities shall be incorporated into the IR procedures.		
Guidance Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.		
Applicability: All	**References:** ARS: IR-4; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4; PISP: 4.8.4	**Related Controls:** AU-6, PE-6, SI-2
ASSESSMENT PROCEDURE: IR-4.1		
Assessment Objective Determine if: (i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and (ii) the incident handling capability is consistent with NIST SP 800-61. **Assessment Methods And Objects** **Examine:** Incident response policy; procedures addressing incident handling; NIST SP 800-61; other relevant documents or records. **Interview:** Organizational personnel with incident handling responsibilities. **Test:** Incident handling capability for the organization.(Optional)		
IR-4(1) – Enhancement (Moderate)		
Control Employ automated mechanisms to support the incident handling process.		
Applicability: All	**References:** ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1)	**Related Controls:**
ASSESSMENT PROCEDURE: IR-4(1).1		
Assessment Objective Determine if the organization employs automated mechanisms to support the incident handling process. **Assessment Methods And Objects** **Examine:** Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; other relevant documents or records. **Interview:** Organizational personnel with incident handling responsibilities.(Optional)		
IR-4(CMS-1) – Enhancement (Moderate)		
Control Document relevant information related to a security incident according to CMS Information Security Incident Handling and Breach Notification Procedures.		
Applicability: All	**References:** ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls:**
ASSESSMENT PROCEDURE: IR-4(CMS-1).1		
Assessment Objective Determine if:		

(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and
(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if relevant information related to a security incident is documented according to the CMS Information Security Incident Handling and Breach Notification Procedures.
Interview: Organizational personnel with incident response training and operational responsibilities to determine if relevant information related to a security incident is documented according to the CMS Information Security Incident Handling and Breach Notification Procedures.

IR-4(CMS-2) – Enhancement (Moderate)

Control

Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.

Applicability: All	**References:** ARS: IR-4(CMS-2); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-4(CMS-2).1

Assessment Objective

Determine if:
(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and
(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if evidence is preserved through technical means, including secured storage of evidence media and "write" protection of evidence media; sound forensics processes and utilities are used that support legal requirements. A chain of custody for forensic evidence is followed.
Interview: Organizational personnel with incident response training and operational responsibilities to determine if evidence is preserved through technical means, including secured storage of evidence media and "write" protection of evidence media; sound forensics processes and utilities are used that support legal requirements. A chain of custody for forensic evidence is followed.

IR-4(CMS-3) – Enhancement (Moderate)

Control

Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure.

Applicability: All	**References:** ARS: IR-4(CMS-3); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-4(CMS-3).1

Assessment Objective

Determine if:
(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and
(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if the identification of vulnerabilities exploited during a security incident and security safeguards are implemented to reduce risk and vulnerability exploit exposure.
Interview: Organizational personnel with incident response training and operational responsibilities to determine if the identification of vulnerabilities exploited during a security incident and security safeguards are implemented to reduce risk and vulnerability exploit exposure.

IR-5 – Incident Monitoring (Moderate)

Control

On-going monitoring of the CMS information system for security events shall be conducted. All events and activities associated with system performance shall be monitored for the identification of resources used by processes and user activity that may indicate security threats resulting from user, software, or hardware activity. All information system security incidents shall be tracked and documented on an on-going basis. All user activities shall be subject to monitoring to verify compliance with this policy and to detect actions that may be in violation of this policy.

Guidance

It is good practice to separate system performance issues from incident tracking. However, unexplained system performance changes can be the result of a security incident occurring or data corruption in transmission within the system. Checksums or cyclic redundancy checks (CRCs) can help during the investigation of these problems. While useful for error detection, CRCs cannot be safely relied upon to fully verify data correctness in the face of deliberate (rather than random) changes.
Remote Procedure Calls (RPCs) can cause performance/incident issues. Note: If an attacker (internal or external person) is able to successfully exploit an RPC vulnerability they could gain complete control over a remote computer. This would give the attacker the ability to take any action on the system that they want. For example, an attacker could change web pages, reformat the hard disk,

and / or add new users to the local administrators group.
Performance and incident tracking on an on-going basis can denote trends within the system or network architecture.

Applicability: All	**References:** ARS: IR-5; FISCAM: TAC-4.2; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#2.3; NIST 800-53/53A: IR-5; PISP: 4.8.5	**Related Controls:**

ASSESSMENT PROCEDURE: IR-5.1

Assessment Objective

Determine if the organization tracks and documents information system security incidents on an ongoing basis.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; other relevant documents or records.
Interview: Organizational personnel with incident monitoring responsibilities.(Optional)
Test: Incident monitoring capability for the organization.(Optional)

IR-6 – Incident Reporting (Moderate)

Control

All IS incidents, or suspected incidents, shall be reported to the CMS IT Service Desk (or equivalent organizational function) as soon as an incident comes to the attention of a user of CMS information or information systems. Events and confirmed security incidents by business partners shall also be reported to the CMS IT Service Desk in accordance with established procedures.

Guidance

The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST SP 800-61 provides guidance on incident reporting.

Applicability: All	**References:** ARS: IR-6; FISCAM: TAC-4.2; NIST 800-53/53A: IR-6; PISP: 4.8.6	**Related Controls:**

ASSESSMENT PROCEDURE: IR-6.1

Assessment Objective

Determine if:
(i) the organization promptly reports incident information to appropriate authorities;
(ii) incident reporting is consistent with NIST SP 800-61;
(iii) the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and
(iv) weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident reporting; NIST SP 800-61; incident reporting records and documentation; other relevant documents or records.
Interview: Organizational personnel with incident reporting responsibilities.
Test: Incident reporting capability for the organization.(Optional)

IR-6(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to assist in the reporting of security incidents.

Applicability: All	**References:** ARS: IR-6(1); NIST 800-53/53A: IR-6(1)	**Related Controls:**

ASSESSMENT PROCEDURE: IR-6(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; other relevant documents or records.
Interview: Organizational personnel with incident reporting responsibilities.(Optional)

IR-7 – Incident Response Assistance (Moderate)

Control

A CMS IT Service Desk (or equivalent organizational function) shall be in place and shall play an appropriate role in the organization's IR program. The CMS IT Service Desk shall offer advice to

users of a CMS information system. Procedures shall be developed, documented, and implemented effectively to facilitate the incident response by providing central incident support resource for CMS information system users.

Guidance

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

Applicability: All	**References:** ARS: IR-7; NIST 800-53/53A: IR-7; PISP: 4.8.7	**Related Controls:**

ASSESSMENT PROCEDURE: IR-7.1

Assessment Objective

Determine if:
(i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and
(ii) the incident response support resource is an integral part of the organization's incident response capability.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; other relevant documents or records.
Interview: Organizational personnel with incident response assistance and support responsibilities.

IR-7(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to increase the availability of incident response-related information and support.

Applicability: All	**References:** ARS: IR-7(1); NIST 800-53/53A: IR-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: IR-7(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support for incident response support.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; other relevant documents or records.
Interview: Organizational personnel with incident response support and assistance responsibilities and organizational personnel that require incident response support and assistance.(Optional)

Maintenance (MA) – *Operational*

MA-1 – System Maintenance Policy and Procedures (Moderate)

Control

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

Guidance

The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: MA-1; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-1; PISP: 4.9.1	**Related Controls:**

ASSESSMENT PROCEDURE: MA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents information system maintenance policy and procedures;
(ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review information system maintenance policy and procedures; and
(iv) the organization updates information system maintenance policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

ASSESSMENT PROCEDURE: MA-1.2

Assessment Objective

Determine if:
(i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-1(FIS-1) – Enhancement (Moderate)

Control

All system software is current, has current and complete documentation, and is still supported by the vendor.

Applicability: All	**References:** FISCAM: TSS-3.2.5, TSS-3.2.6	**Related Controls:**

ASSESSMENT PROCEDURE: MA-1(FIS-1).1

Assessment Objective

Determine if the organization uses current system software with complete documentation and is vendor supported.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Interview: Management and systems programmers about the currency of system software, and the currency and completeness of software documentation.
Interview: System software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.

MA-2 – Controlled Maintenance (Moderate)

Control

Comprehensive maintenance procedures shall be developed, documented, and implemented effectively to conduct controlled periodic on-site and off-site maintenance of the CMS information

systems and of the physical plant within which these information systems reside. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS-approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly.

Guidance

All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Applicability: All; Optional for SS	**References:** ARS: MA-2; FISCAM: TSC-2.4.1, TSC-2.4.2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-2; PISP: 4.9.2	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2.1

Assessment Objective

Determine if the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-2(1) – Enhancement (Moderate)

Control

Maintain maintenance records for each information system that includes:
(a) Date and time of maintenance,
(b) Name of the individual performing the maintenance, name of escort, if applicable,
(c) Description of the maintenance performed, and
(d) List of equipment removed or replaced (including identification numbers, if applicable).

Applicability: All	**References:** ARS: MA-2(1); FISCAM: TSC-2.4.3; NIST 800-53/53A: MA-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2(1).1

Assessment Objective

Determine if the organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records.

MA-2(FIS-1) – Enhancement (Moderate)

Control

Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.

Applicability: All	**References:** FISCAM: TSC-2.4.4	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2(FIS-1).1

Assessment Objective

Determine if the organization accommodates regular and a reasonable amount of unscheduled maintenance in its data processing operations.

Assessment Methods And Objects

Examine: Maintenance documentation.

Examine: Pertinent policies and procedures.

Interview: Data processing and user management.

MA-2(FIS-2) – Enhancement (Moderate)

Control

Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users thus allowing for adequate testing. Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.

Applicability: All	**References:** FISCAM: TSC-2.4.10, TSC-2.4.11	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2(FIS-2).1

Assessment Objective

Determine if:
(i) the organization schedules hardware equipment and related software changes such to minimize user impact and maximize resources for adequate testing; and
(ii) the organizational advance notification for hardware equipment changes does not cause unexpected interrupted user services.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Supporting documentation.
Interview: Senior management, data processing management, and user management.

MA-2(PII-1) – Enhancement (Moderate)

Control

In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Applicability: All	**References:** HIPAA: 164.310(a)(2)(iv)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2(PII-1).1

Assessment Objective

Determine if the organization documents repairs and modifications to the facility containing PII.

Assessment Methods And Objects

Examine: Facility documentation (such as floor plan and elevation drawings) are updated when repairs and modifications cause changes to the physical components of the facility containing PII.
Interview: Organizational personnel, with facility management responsibilities, to determine if facility documents reflect security changes caused by repairs and modifications.
Test: Facility documentation sample to determine if repairs or modifications document physical security implications when the facility is protecting PII.

MA-3 – Maintenance Tools (Moderate)

Control

The use of system maintenance tools, including diagnostic and test equipment and administration utilities, shall be approved, controlled, and monitored. Approved tools shall be maintained on an on-going basis.

Guidance

The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Applicability: All	**References:** ARS: MA-3; IRS-1075: 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-3; PISP: 4.9.3	**Related Controls:**

ASSESSMENT PROCEDURE: MA-3.1

Assessment Objective

Determine if:
(i) the organization approves, controls, and monitors the use of information system maintenance tools; and
(ii) the organization maintains maintenance tools on an ongoing basis.

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.

MA-4 – Remote Maintenance (Moderate)

Control

Remote maintenance of a CMS information system must be approved by the CIO or his/her designated representative. Remote maintenance procedures shall be developed, documented, and implemented effectively to provide additional controls on remotely executed maintenance and diagnostic activities.

The use of remote diagnostic tools shall be described in the SSP for the information system. Maintenance records for all remote maintenance, diagnostic, and service activities shall be maintained and shall be reviewed periodically by appropriate organization officials. All sessions and remote connections shall be terminated after the remote maintenance is completed. If password-based authentication is used during remote maintenance, the passwords shall be changed following each remote maintenance service.

Guidance

Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST SP 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Applicability: All	**References:** ARS: MA-4; FISCAM: TAC-2.1.3; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4; PISP: 4.9.4	**Related Controls:** IA-2, MP-6

ASSESSMENT PROCEDURE: MA-4.1

Assessment Objective

Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-4(1) – Enhancement (Moderate)

Control

Audit all remote maintenance sessions, and ensure that appropriate information security personnel review the maintenance records of the remote sessions.

Applicability: All	**References:** ARS: MA-4(1); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-4(1).1

Assessment Objective

Determine if:

(i) the organization audits all remote maintenance and diagnostic sessions; and

(ii) designated organizational personnel review the maintenance records of remote sessions.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; maintenance records; audit records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-4(2) – Enhancement (Moderate)

Control

Document the use of remote diagnostic tools in the SSP.

Applicability: All	**References:** ARS: MA-4(2); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4(2)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-4(2).1

Assessment Objective

Determine if the organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; information system security plan; maintenance records; audit records; other relevant documents or records.

MA-4(CMS-1) – Enhancement (Moderate)

Control

If remote maintenance is authorized in writing by the CIO or his/her designated representative:
Encrypt and decrypt diagnostic communications; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, terminate all sessions and remote connections. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.

Applicability: All	**References:** ARS: MA-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-4(CMS-1).1

Assessment Objective

Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that remote maintenance is authorized in writing by the CIO or his/her designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service.

Interview: Organizational personnel with information system maintenance responsibilities to determine that remote maintenance is authorized in writing by the CIO or his/her designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service.

MA-5 – Maintenance Personnel (Moderate)

Control

Maintenance personnel procedures shall be developed, documented, and implemented effectively to control maintenance of CMS information systems. A list of individuals authorized to perform maintenance on the information system shall be maintained.

Guidance

Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Applicability: All	**References:** ARS: MA-5; NIST 800-53/53A: MA-5; PISP: 4.9.5	**Related Controls:**

ASSESSMENT PROCEDURE: MA-5.1

Assessment Objective

Determine if the organization allows only authorized personnel to perform maintenance on the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-5(0) – Enhancement (Moderate)

Control

Only authorized individuals are allowed to perform maintenance. Ensure maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. Supervise maintenance personnel during the performance of maintenance activities when they do not have the needed access authorizations.

Applicability: All	**References:** ARS: MA-5(0); HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: MA-5; PISP: 4.9.5	**Related Controls:**

ASSESSMENT PROCEDURE: MA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-6 – Timely Maintenance (Moderate)

Control

Maintenance services and parts shall be available in a timely manner.

Guidance

It is good practice to determine the priority of each system based on the criticality of the system for continued business operations. Each system should be prioritized and interconnections between each of the enterprise's systems mapped and dataflow diagrams developed.
Next maintenance contracts as well as emergency maintenance considerations will determine needed availability and pre-placement of spare parts.

Applicability: All	References: ARS: MA-6; NIST 800-53/53A: MA-6; PISP: 4.9.6	Related Controls:

ASSESSMENT PROCEDURE: MA-6.1

Assessment Objective

Determine if:
(i) the organization defines key information system components;
(ii) the organization defines the time period within which support and spare parts must be obtained after a failure; and
(iii) the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.

MA-6(0) – Enhancement (Moderate)

Control

Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twenty-four (24) hours of failure.

Applicability: All	References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6	Related Controls:

ASSESSMENT PROCEDURE: MA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts must be obtained after a failure); other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.

MA-CMS-1 – Off-site Physical Repair of Systems (Moderate)

Control

Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality.

Guidance

It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approved Change Management baseline.
Storage media control when encrypted may take special considerations.

Applicability: All	References: ARS: MA-CMS-1; PISP: 4.9.7	Related Controls: AC-19(CMS-1), AC-3, CP-9, SC-12(CMS-1)

ASSESSMENT PROCEDURE: MA-CMS-1.1

Assessment Objective

Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair.
Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.

MA-CMS-1(CMS-0) – Enhancement (Moderate)		
Control Access to system for repair must be by authorized personnel only. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, check security features to verify they are functioning properly.		
Applicability: All	**References:** ARS: MA-CMS-1(CMS-0); HIPAA: 164.310(d)(2)(i)	**Related Controls:**
ASSESSMENT PROCEDURE: MA-CMS-1(CMS-0).1		
Assessment Objective Determine if the organization allows only authorized personnel perform maintenance on the information system. **Assessment Methods And Objects** **Examine:** Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for repair. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, security features are checked to verify they are functioning properly. **Interview:** Organizational personnel with information system maintenance responsibilities determine that only authorized personnel are permitted access to system for repair. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, security features are checked to verify they are functioning properly.		
MA-CMS-2 – On-site Physical Repair of Systems (Moderate)		
Control Controls shall be developed, documented, and implemented effectively to enable on-site physical repair of systems without compromising security functionality or confidentiality.		
Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has completed repairs. The repaired system should match the approved Change Management baseline. Storage media control when encrypted may take special considerations.		
Applicability: All	**References:** ARS: MA-CMS-2; PISP: 4.9.8	**Related Controls:** AC-19(CMS-1), AC-3, CP-9, SC-12(CMS-1)
ASSESSMENT PROCEDURE: MA-CMS-2.1		
Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements on-site repair of systems without compromising security functionality or confidentiality. **Assessment Methods And Objects** **Examine:** Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for on-site repair. **Interview:** Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during on-site repair.		
MA-CMS-2(CMS-1) – Enhancement (Moderate)		
Control Access to system for repair must be by authorized personnel only.		
Applicability: All	**References:** ARS: MA-CMS-2(CMS-1)	**Related Controls:**
ASSESSMENT PROCEDURE: MA-CMS-2(CMS-1).1		
Assessment Objective Determine if the organization allows only authorized personnel perform maintenance on the information system. **Assessment Methods And Objects** **Examine:** Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel perform maintenance on the information system. **Interview:** Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel perform maintenance on the information system.		
MA-CMS-2(CMS-2) – Enhancement (Moderate)		
Control Physical repair of servers must be within protected environments.		
Applicability: All	**References:** ARS: MA-CMS-2(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-CMS-2(CMS-2).1

Assessment Objective

Determine if the organization performs physical repair of servers within protected environments.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine physical repair of servers is performed within protected environments.

Interview: Organizational personnel with information system maintenance responsibilities to determine physical repair of servers is performed within protected environments.

Media Protection (MP) – *Operational*

MP-1 – Media Protection Policy and Procedures (Moderate)

Control

MP controls and procedures shall be developed, documented, and implemented effectively to address media access; media labeling; media transport; media destruction; media sanitization and clearing; media storage; and disposition of media records. The MP procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: MP-1; FISCAM: TAC-3.4; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1; NIST 800-53/53A: MP-1; PISP: 4.10.1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents media protection policy and procedures;
(ii) the organization disseminates media protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review media protection policy and procedures; and
(iv) the organization updates media protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.(Optional)

ASSESSMENT PROCEDURE: MP-1.2

Assessment Objective

Determine if:
(i) the media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.(Optional)

MP-1(PII-1) – Enhancement (Moderate)

Control

Semiannual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss.

Applicability: All	**References:** IRS-1075: 3.2#3.2, 3.2#3.3	**Related Controls:**

ASSESSMENT PROCEDURE: MP-1(PII-1).1

Assessment Objective

Determine if:
(i) the organization verifies semiannual inventories of magnetic tapes containing PII.
(ii) the organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss.

Assessment Methods And Objects

Examine: Records of semiannual inventories of PII magnetic tapes conducted. If tapes are missing the initiator is notified and a record of the investigation is documented.

MP-2 – Media Access (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media based on the sensitivity of the CMS information. Automated mechanisms shall be implemented to control access to media storage areas and to audit

access attempts and access granted.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Applicability: All	**References:** ARS: MP-2; FISCAM: TAC-3.1.A.6, TAY-4.1.1; HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1; NIST 800-53/53A: MP-2; PISP: 4.10.2	**Related Controls:**

ASSESSMENT PROCEDURE: MP-2.1

Assessment Objective

Determine if the organization restricts access to information system media to authorized users.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records.

Interview: Organizational personnel with information system media protection responsibilities.

MP-2(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Guidance

This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

Applicability: All	**References:** ARS: MP-2(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.5; IRS-1075: 4.6#1; NIST 800-53/53A: MP-2(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MP-2(1).1

Assessment Objective

Determine if:

(i) the organization employs automated mechanisms to restrict access to media storage areas; and

(ii) the organization employs automated mechanisms to audit access attempts and access granted.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records.

Test: Automated mechanisms implementing access restrictions to media storage areas.(Optional)

MP-3 – Media Labeling (Moderate)

Control

Storage media and information system output shall have external labels affixed to indicate the distribution limitations, applicable security classification, and handling caveats of the information. Specific types of media or hardware components may be exempted from the labeling requirement, so long as the exempted items remain within a secure environment. Only the CIO or his/her designated representative shall have the authority to exempt specific types of media or hardware components from the labeling requirement.

Guidance

An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Applicability: All	**References:** ARS: MP-3; IRS-1075: 4.6#1, 5.1#1.2, 5.3#2.1-2, 5.3#3; NIST 800-53/53A: MP-3; PISP: 4.10.3	**Related Controls:**

ASSESSMENT PROCEDURE: MP-3.1

Assessment Objective

Determine if:
(i) the organization defines its protected environment for media labeling requirements;
(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;
(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and
(iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; information system security plan; removable storage media and information system output; other relevant documents or records.(Optional)

MP-3(CMS-1) – Enhancement (Moderate)

Control

Off-line backup storage media must be marked according to backup rotation schedule for ease of retrieval.

Applicability: All	**References:** ARS: MP-3(CMS-1); IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-3(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines its protected environment for media labeling requirements;
(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;
(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and
(iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine that off-line backup storage media is marked according to backup rotation schedule for ease of retrieval.

Interview: Organizational personnel with information system media protection responsibilities to determine off-line backup storage media is marked according to backup rotation schedule for ease of retrieval.

MP-4 – Media Storage (Moderate)

Control

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper, within controlled areas. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security level of the information ever recorded on it until destroyed or sanitized using CMS-approved procedures.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST SP 800-56 and 800-57 provide guidance on cryptographic key

establishment and cryptographic key management.

Applicability: All	References: ARS: MP-4; FISCAM: TCC-3.2.4, TCC-3.3.1; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1; NIST 800-53/53A: MP-4; PISP: 4.10.4	Related Controls: AC-19, CP-9, CP-9(4), RA-2, SC-7

ASSESSMENT PROCEDURE: MP-4.1

Assessment Objective

Determine if:
(i) the organization defines controlled areas for information system media;
(ii) the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk;
(iii) the organization defines the specific measures used to protect the selected media and information contained on that media;
(iv) the organization physically controls and securely stores information system media within controlled areas; and
(v) the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media; other relevant documents or records.

MP-4(PII-1) – Enhancement (Moderate)

Control

Evaluate employing an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest, consistent with NIST SP 800-66 guidance.

Applicability: All	References: HIPAA: 164.312(a)(2)(iv)	Related Controls: SC-13

ASSESSMENT PROCEDURE: MP-4(PII-1).1

Assessment Objective

Determine if the organization uses approved cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest.

Assessment Methods And Objects

Examine: Cryptographic software licenses used to protect PII at rest. Cryptography software is consistent with NIST SP 800-66 guidance and FIPS 140 approved.
Interview: Organizational staff to determine if FIPS 140 approved cryptographic software/system for PII data at rest protection is being used.

MP-4(PII-2) – Enhancement (Moderate)

Control

If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information.

Applicability: All	References: IRS-1075: 5.3#2.3, 5.3#3	Related Controls:

ASSESSMENT PROCEDURE: MP-4(PII-2).1

Assessment Objective

Determine if the organization protects, in its entirety, personally identifiable information when on magnetic media with other data.

Assessment Methods And Objects

Examine: Magnetic storage of PII is protected to determine, in its entirety, it is controlled as Federal tax information.
Interview: Organizational staff to determine if PII in its entirety is protected as personally identifiable information.

MP-5 – Media Transport (Moderate)

Control

Physical, administrative, and technical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) to authorized personnel based on the sensitivity of the CMS information.

Guidance

Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with

the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Applicability: All	**References:** ARS: MP-5; FISCAM: TAY-4.1.1, TAY-4.1.4; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.6#2, 4.6#4; NIST 800-53/53A: MP-5; PISP: 4.10.5	**Related Controls:** AC-19, CP-9, CP-9(4)

ASSESSMENT PROCEDURE: MP-5.1

Assessment Objective

Determine if:
(i) the organization identifies personnel authorized to transport information system media outside of controlled areas;
(ii) the organization controls information system media during transport outside of controlled areas; and
(iii) the organization restricts the activities associated with transport of information system media to authorized personnel.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records.

MP-5(1) – Enhancement (Moderate)

Control

All sensitive information stored on digital media are protected during transport outside of controlled areas by using cryptography and tamper proof packaging and (a) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier.
If the use of cryptography is not technically feasible or the sensitive information is stored on non-digital media, written management approval (one level below the CIO) must be obtained prior to transport and the information must be (a) hand carried using securable container via authorized personnel, or (b) if shipped, by United States Postal Service (USPS) Certified Mail with return receipt in tamper-proof packaging.
Correspondence pertaining to a single individual may be mailed through regular USPS mail, but should contain only the minimal amount of sensitive information in order to reduce the risk of unauthorized disclosure (e.g., partially masking social security numbers).

Guidance

Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used.

Applicability: All	**References:** ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1)	**Related Controls:**

ASSESSMENT PROCEDURE: MP-5(1).1

Assessment Objective

Determine if:
(i) the organization defines security measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas; and
(ii) the organization protects digital and non-digital media during transport outside of controlled areas using the organization-defined security measures.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media transport records; audit records; other relevant documents or records.
Interview: Organizational personnel with information system media transport responsibilities.(Optional)

MP-5(2) – Enhancement (Moderate)

Control

Activities associated with the transport of sensitive information system media are documented.

Guidance

Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

Applicability: All	**References:** ARS: MP-5(2); IRS-1075: 3.2#3.1, 4.4#2, 4.6#2; NIST 800-53/53A: MP-5(2)	**Related Controls:**

ASSESSMENT PROCEDURE: MP-5(2).1

Assessment Objective

Determine if:

(i) the organization defines a system of records for documenting activities associated with the transport of information system media; and
(ii) the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media transport records; audit records; other relevant documents or records.

MP-5(PII-1) – Enhancement (Moderate)

Control

Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.

Applicability: All	**References:** IRS-1075: 4.4#1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-5(PII-1).1

Assessment Objective

Determine if:
(i) the organization protects and controls PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel; and
(ii) the organization uses locked cabinets or sealed packing cartons while PII data is in transit.

Assessment Methods And Objects

Examine: Rosters or list of authorized personnel to protect and control PII media during transit.
Examine: Cabinets or the containers used for protecting PII during transit to determine if there is sufficient fortification to protect PII.

MP-6 – Media Sanitization and Disposal (Moderate)

Control

Formal documented procedures shall be developed and implemented effectively to ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of data residing on storage devices, equipment, and hard copy documents. Media sanitization actions shall be tracked, documented, and verified. Sanitization equipment and procedures shall be tested periodically to ensure proper functionality.

Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmentally approved manner, to facilitate the disposal of media, both electronic and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. Approved equipment removal procedures for CMS information systems and components that have processed or contained CMS information shall be followed. Inventory and disposition records for media, both electronic and paper, shall be produced, stored, updated, and retained.

Guidance

Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Applicability: All	**References:** ARS: MP-6; FISCAM: TAC-3.4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-1075: 4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2; NIST 800-53/53A: MP-6; PISP: 4.10.6	**Related Controls:** MA-4

ASSESSMENT PROCEDURE: MP-6.1

Assessment Objective

Determine if:
(i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process;
(ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and
(iii) information system media sanitation is consistent with NIST SP 800-88.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization records; audit records; other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

MP-6(0) – Enhancement (Moderate)		
Control The sanitization process includes the removal of all data, labels, marking, and activity records using NSA Guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, Guidelines for Media Sanitization.		
Applicability: All	**References:** ARS: MP-6(0); FISCAM: TAC-3.4; IRS-1075: 8.4#2, 8.4#3; NIST 800-53/53A: MP-6; PISP: 4.10.6	**Related Controls:**
ASSESSMENT PROCEDURE: MP-6(0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization records; audit records; other relevant documents or records. **Interview:** Organizational personnel with information system media sanitization responsibilities.		
MP-6(CMS-1) – Enhancement (Moderate)		
Control Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.		
Applicability: All	**References:** ARS: MP-6(CMS-1)	**Related Controls:**
ASSESSMENT PROCEDURE: MP-6(CMS-1).1		
Assessment Objective Determine if: (i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process; (ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and (iii) information system media sanitation is consistent with NIST SP 800-88. **Assessment Methods And Objects** **Examine:** Media protection policy and procedures; other relevant documents or records to determine hard copy documents are finely shred, using a minimum of cross-cut shredding, using approved equipment, techniques, and procedures. **Interview:** Organizational personnel with information system media protection responsibilities to determine hard copy documents are finely shred, using a minimum of cross-cut shredding, using approved equipment, techniques, and procedures.		
MP-6(IRS-1) – Enhancement (Moderate)		
Control FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee.		
Applicability: All	**References:** IRS-1075: 8.4#1	**Related Controls:**
ASSESSMENT PROCEDURE: MP-6(IRS-1).1		
Assessment Objective Determine if: (i) the organization never discloses FTI to the agency's agents or contractors during disposal unless authorized by the Internal Revenue Code; and (ii) the organization, generally, uses an agency employee to witness FTI destruction. **Assessment Methods And Objects** **Examine:** FTI disposal records to determine if unauthorized disclose has been given to contractors or other agency agents.		
MP-CMS-1 – Media Related Records (Moderate)		
Control Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.		
Guidance It is good practice for, electronic, inventory records maintenance that a hash function (a reproducible method of turning inventory data into a (relatively) small number that may serve as a digital "fingerprint" of the data) be performed periodically so that the inventory information can be validated as not being tampered with prior to reconstructive events for an investigation of a possible breach.		

Applicability: All	References: ARS: MP-CMS-1; FISCAM: TCC-3.2.4; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4; PISP: MP-CMS-1	Related Controls:

ASSESSMENT PROCEDURE: MP-CMS-1.1

Assessment Objective

Determine if the organization maintains inventory and disposition records for information system media to ensure control and accountability of CMS information.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information.

Interview: Organizational personnel with information system media protection responsibilities to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information.

MP-CMS-1(CMS-0) – Enhancement (Moderate)

Control

The media records must, at a minimum, contain:
(a) The name of media recipient;
(b) Signature of media recipient;
(c) Date / time media received;
(d) Media control number and contents;
(e) Movement or routing information; and
(f) If disposed of, the date, time, and method of destruction.

Applicability: All	References: ARS: MP-CMS-1(CMS-0); FISCAM: TCC-3.2.4; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4	Related Controls:

ASSESSMENT PROCEDURE: MP-CMS-1(CMS-0).1

Assessment Objective

Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information. The media records shall contain sufficient information to reconstruct the data in the event of a breach, including but not limited to:
(a) the name of media recipient;
(b) signature of media recipient;
(c) date / time media received;
(d) media control number and contents;
(e) movement or routing information; and
(f) if disposed of, the date, time, and method of destruction.

Interview: Organizational personnel with information system media protection responsibilities to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information. The media records shall contain sufficient information to reconstruct the data in the event of a breach, including but not limited to:
(a) the name of media recipient;
(b) signature of media recipient;
(c) date / time media received;
(d) media control number and contents;
(e) movement or routing information; and
(f) if disposed of, the date, time, and method of destruction.

MP-CMS-1(PII-1) – Enhancement (Moderate)

Control

For PII, authorized employees of the recipient must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:
• date received
• reel/cartridge control number contents
• number of records, if available
• movement, and

• if disposed of, the date and method of disposition.

Applicability: All	References: IRS-1075: 3.2#1	Related Controls:

ASSESSMENT PROCEDURE: MP-CMS-1(PII-1).1

Assessment Objective

Determine if:
(i) the organization documents the securing of PII magnetic tapes/cartridges before, during, and after processing, and the proper acknowledgment form is signed and returned; and
(ii) the organizational inventory records maintain PII control and accountability by a log which contains:
• date received
• reel/cartridge control number contents
• number of records, if available
• movement, and
• if disposed of, the date and method of disposition.

Assessment Methods And Objects

Examine: The PII inventory tape/cartridge log for:
• date received
• reel/cartridge control number contents
• number of records, if available
• movement, and
• if disposed of, the date and method of disposition.

MP-CMS-1(IRS-1) – Enhancement (Moderate)

Control

For FTI, organizations are not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7)

Applicability: All	References: IRS-1075: 11.1#1	Related Controls:

ASSESSMENT PROCEDURE: MP-CMS-1(IRS-1).1

Assessment Objective

Determine if the organization allows unauthorized disclosure of FTI data to their agents or to an unauthorized contractor.

Assessment Methods And Objects

Examine: FTI disclosure documentation to determine is authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7)
Interview: Organizational staff to determine if personnel are knowledgeable of IRS Pub. 1075, sect. 11.1 and 11.7 regarding disclosure of FTI data.

Physical and Environmental Protection (PE) – *Operational*

PE-1 – Physical and Environmental Protection Policy and Procedures (Moderate)

Control

Physical and environmental protection procedures shall be developed and implemented effectively to protect all CMS IT infrastructure and assets from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional. These procedures shall meet all federal, state and local building codes and be consistent with General Services Administration policies, directives, regulations, and guidelines.

Guidance

The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: PE-1; FISCAM: TSC-2.2.6, TSC-2.3.4, TSD-2.1; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1; NIST 800-53/53A: PE-1; PISP: 4.11.1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents physical and environmental protection policy and procedures;
(ii) the organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review physical and environmental protection policy and procedures; and
(iv) the organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Physical and environmental protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with physical and environmental protection responsibilities.(Optional)

ASSESSMENT PROCEDURE: PE-1.2

Assessment Objective

Determine if:
(i) the physical and environmental protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Physical and environmental protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with physical and environmental protection responsibilities.(Optional)

PE-1(FIS-1) – Enhancement (Moderate)

Control

Eating, drinking, and other behavior that may damage computer equipment is prohibited.

Applicability: All	**References:** FISCAM: TSC-2.2.7	**Related Controls:**

ASSESSMENT PROCEDURE: PE-1(FIS-1).1

Assessment Objective

Determine if the organization prohibits eating, drinking, and other behavior that may damage computer equipment.

Assessment Methods And Objects

Examine: Employee behavior.
Examine: Employee rules of behavior.
Examine: Pertinent policies and procedures.
Interview: Information system management and users.

PE-2 – Physical Access Authorizations (Moderate)

Control

Access lists of personnel with authorized access to facilities containing CMS information or information systems (except for those areas within the facilities officially designated as publicly accessible) shall be documented on standard forms, maintained on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessary, updated. Appropriate authorization credentials (e.g., badges, identification cards, smart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be removed promptly from all access lists.

Guidance

Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides.

Applicability: All	**References:** ARS: PE-2; FISCAM: TAC-2.1.1, TAC-2.1.2, TAC-2.1.4, TAC-2.2, TAC-3.1.A.3, TAC-3.1.A.4, TAC-3.1.A.8, TSS-1.2.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	**Related Controls:**

ASSESSMENT PROCEDURE: PE-2.1

Assessment Objective

Determine if:
(i) the organization identifies areas within the facility that are publicly accessible;
(ii) the organization defines the frequency of review and approval for the physical access list and authorization credentials for the facility;
(iii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
(iv) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and
(v) designated officials within the organization review and approve the access list and authorization credentials at the organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records.

PE-2(0) – Enhancement (Moderate)

Control

Review and approve lists of personnel with authorized access to facilities containing information systems at least once every 180 days.

Applicability: All	**References:** ARS: PE-2(0); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-3.1.A.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	**Related Controls:**

ASSESSMENT PROCEDURE: PE-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records.

PE-2(PII-1) – Enhancement (Moderate)

Control

Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.

Applicability: All	**References:** IRS-1075: 4.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-2(PII-1).1

Assessment Objective

Determine if:
(i) the organization created a restricted area, security room, or locked room to control access to areas containing PII; and
(ii) the organization controls a restricted area, security room, or locked room in accordance with BPSSM.

Assessment Methods And Objects

Examine: Restricted areas, security rooms, or locked rooms that control access to areas containing PII to determine if control and fortification functions are in accordance with BPSSM.
Interview: Facility personnel responsible for controlling restricted areas, security rooms, or locked rooms containing PII to determine compliance with BPSSM.

PE-3 – Physical Access Control (Moderate)

Control

Physical access control devices (e.g., keys, locks, combinations, card-readers) and/or guards shall be used to control entry to and exit from facilities containing CMS information or information systems, except for areas and/or facilities officially designated as publicly accessible. Individual access authorizations shall be verified before granting access to facilities containing CMS information or information systems. Physical access control devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis.

Combinations, access codes, and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry to facilities during emergency-related events shall be restricted to authorized individuals only. Access to workstations and associated peripheral computing devices shall be appropriately controlled when located in areas designated as publicly accessible.

Guidance

The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST SP 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST SP 800-76.

Applicability: All	**References:** ARS: PE-3; FISCAM: TAC-3.1.A.3, TAC-3.1.A.5, TAC-3.1.A.7, TAC-3.1.A.8, TAC-3.1.B.2, TAN-2.1.1, TAN-2.1.2, TAN-2.2.1, TSD-2.1; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1; NIST 800-53/53A: PE-3; PISP: 4.11.3	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3.1

Assessment Objective

Determine if:
(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
(ii) the organization verifies individual access authorizations before granting access to the facility; and
(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records.
Interview: Organizational personnel with physical access control responsibilities.(Optional)
Test: Physical access control capability.

ASSESSMENT PROCEDURE: PE-3.2

Assessment Objective

Determine if:
(i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis;
(ii) the organization secures keys, combinations and other access devices on a regular basis; and
(iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records.
Test: Physical access control devices.

ASSESSMENT PROCEDURE: PE-3.3

Assessment Objective

Determine if:
(i) the access control system is consistent with FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed);
(ii) the access control system is consistent with NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and
(iii) the access control system is consistent with NIST SP 800-76 (where the token-based access control function employs biometric verification).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST SP 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records.

Test: Physical access control devices.

PE-3(CMS-1) – Enhancement (Moderate)

Control

Control data center / facility access by use of door and window locks, and security staff or physical authentication devices, such as biometrics and/or smart card / PIN combination.

Applicability: All	**References:** ARS: PE-3(CMS-1); IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-1).1

Assessment Objective

Determine if the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine data center / facility access is controlled by use of door and window locks.

Interview: Organizational personnel with physical access control responsibilities to confirm data center / facility access is controlled by use of door and window locks.

Test: Physical access control capability to determine data center / facility access is controlled by use of door and window locks.

PE-3(CMS-2) – Enhancement (Moderate)

Control

Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.

Applicability: All	**References:** ARS: PE-3(CMS-2); FISCAM: TAC-3.1.A.5; IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-2).1

Assessment Objective

Determine if the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine servers are stored and operated in physically secure environments protected from unauthorized access.

Interview: Organizational personnel with physical access control responsibilities to determine servers are stored and operated in physically secure environments protected from unauthorized access.

Test: Physical access to Data Center to determine servers are stored and operated in physically secure environments protected from unauthorized access.

PE-3(CMS-3) – Enhancement (Moderate)

Control

Data centers must meet the minimum requirements as established by the Federal Information Systems Control Audit Manual (FISCAM).

Applicability: All	**References:** ARS: PE-3(CMS-3); FISCAM: TAC-3.1.A.1, TAN-2.1.1, TAN-2.1.2; IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-3).1

Assessment Objective

Determine if:

(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

(ii) the organization verifies individual access authorizations before granting access to the facility; and

(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if data centers meet the minimum requirements as established by the Federal Information Systems Control Audit Manual (FISCAM).

PE-3(CMS-4) – Enhancement (Moderate)

Control

Restrict access to grounds / facilities to authorized persons only.

Applicability: All	References: ARS: PE-3(CMS-4); IRS-1075: 4.6#1	Related Controls:

ASSESSMENT PROCEDURE: PE-3(CMS-4).1

Assessment Objective

Determine if the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if access to grounds / facilities is restricted to authorized persons only.

Interview: Organizational personnel with physical access control responsibilities to determine access to grounds / facilities is restricted to authorized persons only.

Test: Physical access controls to determine if access to grounds / facilities is restricted to authorized persons only.

PE-3(PII-1) – Enhancement (Moderate)

Control

For PII, require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access after hours.

Applicability: All	References: IRS-1075: 4.2#2	Related Controls:

ASSESSMENT PROCEDURE: PE-3(PII-1).1

Assessment Objective

Determine if:

(i) the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; and

(ii) the organization containerizes protected information in areas where other than authorized employees may have access after hours.

Assessment Methods And Objects

Examine: Barriers to protect PII to determine two (2) barriers are present for normal security.

Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours.

Interview: Organizational personnel to determine if PII has been disclosed to unauthorized employees.

Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel.

PE-3(DIR-1) – Enhancement (Moderate)

Control

Controls are established to protect access authorization lists to secure areas such as data centers.

Applicability: All	References:	Related Controls:

ASSESSMENT PROCEDURE: PE-3(DIR-1).1

Assessment Objective

Determine if the organization protects approved access authorization lists that are for secure areas.

Assessment Methods And Objects

Examine: Protection procedures are in place for approved access authorization lists to secure areas.

PE-4 – Access Control for Transmission Medium (Moderate)

Control

Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering of CMS information system transmission lines within organizational facilities that carry unencrypted information.

Guidance

Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Applicability: All	References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4	Related Controls:

ASSESSMENT PROCEDURE: PE-4.1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records.(Optional)

PE-4(CMS-1) – Enhancement (Moderate)

Control

Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel.

Applicability: All	**References:** ARS: PE-4(CMS-1); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-4(CMS-1).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

Interview: Organizational personnel with physical access control responsibilities to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

Test: Physical access controls to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

PE-4(CMS-2) – Enhancement (Moderate)

Control

Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use.

Applicability: All	**References:** ARS: PE-4(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-4(CMS-2).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

Interview: Organizational personnel with physical access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

Test: Physical access controls to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

PE-5 – Access Control for Display Medium (Moderate)

Control

Physical access controls shall be developed, documented, and implemented effectively to prevent unauthorized individuals from observing CMS sensitive information displayed on information system devices.

Guidance

It is good practice to position sensitive information display devices away from windows and areas of ingress and egress.

Applicability: All	**References:** ARS: PE-5; FISCAM: TAN-2.1.1; HIPAA: 164.310(b); NIST 800-53/53A: PE-5; PISP: 4.11.5	**Related Controls:**

ASSESSMENT PROCEDURE: PE-5.1

Assessment Objective

Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; other relevant documents or records.

PE-6 – Monitoring Physical Access (Moderate)

Control

Physical access to information systems shall be monitored for physical security compliance and to detect and respond to incidents. Appropriate organization officials shall periodically review physical

access records, investigate apparent security violations or suspicious physical access activities, and take appropriate remedial action.

Guidance

The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.

Applicability: All	**References:** ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN-2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6	**Related Controls:** IR-4

ASSESSMENT PROCEDURE: PE-6.1

Assessment Objective

Determine if the organization monitors physical access to the information system to detect and respond to physical security incidents.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; other relevant documents or records.

Interview: Organizational personnel with physical access monitoring responsibilities.

Test: Physical access monitoring capability.

PE-6(1) – Enhancement (Moderate)

Control

Monitor real-time physical intrusion alarms and surveillance equipment.

Applicability: All	**References:** ARS: PE-6(1); NIST 800-53/53A: PE-6(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-6(1).1

Assessment Objective

Determine if the organization monitors real-time intrusion alarms and surveillance equipment.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; intrusion alarm/surveillance equipment logs or records; other relevant documents or records.

Interview: Organizational personnel with physical access monitoring responsibilities.(Optional)

PE-7 – Visitor Control (Moderate)

Control

Visitor controls shall be developed, documented, and implemented effectively to control access to sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries. Visitors shall be authenticated prior to being granted access to facilities or areas other than areas designated as publicly accessible. Government contractors and others with permanent authorization credentials are not considered visitors.

Guidance

Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST SP 800-79.

Applicability: All	**References:** ARS: PE-7; FISCAM: TAC-3.1.B.3; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7; PISP: 4.11.7	**Related Controls:**

ASSESSMENT PROCEDURE: PE-7.1

Assessment Objective

Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.

Interview: Organizational personnel with visitor access control responsibilities.(Optional)

Test: Visitor access control capability.

PE-7(1) – Enhancement (Moderate)

Control

Escort visitors and monitor visitor activity.

Applicability: All	**References:** ARS: PE-7(1); FISCAM: TAC-3.1.B.1; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-7(1).1

Assessment Objective

Determine if the organization escorts visitors and monitors visitor activity, when required.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.

Interview: Organizational personnel with visitor access control responsibilities.(Optional)

PE-7(FIS-1) – Enhancement (Moderate)

Control

Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.

Applicability: All	**References:** FISCAM: TAC-3.1.B.3	**Related Controls:**

ASSESSMENT PROCEDURE: PE-7(FIS-1).1

Assessment Objective

Determine if the organization authenticates visitors, contractors and maintenance personnel through the use of preplanned appointments and identification checks.

Assessment Methods And Objects

Examine: Appointment and verification procedures for visitors.

Examine: Pertinent policies and procedures.

Interview: Receptionist or security guard.

PE-8 – Access Records (Moderate)

Control

Visitor access to sensitive facilities and restricted / controlled areas that contain CMS information or information systems shall be logged. The visitor access record shall contain:

4.11.8.1. Name and organization of the person visiting;
4.11.8.2. Signature of the visitor;
4.11.8.3. Form of identification;
4.11.8.4. Date of access;
4.11.8.5. Time of entry and departure;
4.11.8.6. Purpose of visit; and
4.11.8.7. Name and organization of person visited.

Appropriate organization officials shall periodically review the access records, including after closeout.

Guidance

It is good practice to have a standard log format for consistency and ease of use during log closeouts and the next months log generation.

Applicability: All	**References:** ARS: PE-8; FISCAM: TAC-3.1.B.1, TAC-3.1.B.3; NIST 800-53/53A: PE-8; PISP: 4.11.8	**Related Controls:**

ASSESSMENT PROCEDURE: PE-8.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of review for visitor access records;
(ii) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes:
- name and organization of the person visiting;
- signature of the visitor;
- form of identification;
- date of access;
- time of entry and departure;
- purpose of visit;
- name and organization of person visited and

(iii) designated officials within the organization review the visitor access logs in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan; facility access control records; other relevant documents or

records.

PE-8(0) – Enhancement (Moderate)

Control

Visitor access records must be closed out and reviewed by management monthly.

Applicability: All	**References:** ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8	**Related Controls:**

ASSESSMENT PROCEDURE: PE-8(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan (for organization-defined frequency for review of visitor access records); facility access control records; other relevant documents or records.

PE-9 – Power Equipment and Power Cabling (Moderate)

Control

Power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain safe power for CMS information systems.

Guidance

Both primary and backup power systems should be included in the safe power implementation procedures. Remote backup site's power implementation should be included in the documentation.

Applicability: All	**References:** ARS: PE-9; NIST 800-53/53A: PE-9; PISP: 4.11.9	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9.1

Assessment Objective

Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.

PE-9(CMS-1) – Enhancement (Moderate)

Control

Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

Applicability: All	**References:** ARS: PE-9(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9(CMS-1).1

Assessment Objective

Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

Interview: Organizational personnel with physical access control responsibilities to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

PE-9(CMS-2) – Enhancement (Moderate)

Control

Power surge protection must be implemented for all computer equipment.

Applicability: All	**References:** ARS: PE-9(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9(CMS-2).1

Assessment Objective

Determine if the organization protects power equipment and implements surge protection for all computers to assist in protection from damage or destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents /records / diagrams to determine if power surge protection is implemented for all computer equipment.

Interview: Organizational personnel with physical access control responsibilities to determine if power surge protection is implemented for all computer equipment.

Test: Verify by physical inspection to determine if power surge protection is implemented for all computer equipment.

PE-10 – Emergency Shutoff (Moderate)

Control

Emergency shut-off controls shall be developed, documented, and implemented effectively to provide the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

Guidance

Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Applicability: All	**References:** ARS: PE-10; NIST 800-53/53A: PE-10; PISP: 4.11.10	**Related Controls:**

ASSESSMENT PROCEDURE: PE-10.1

Assessment Objective

Determine if:
(i) the organization defines the specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms); and
(ii) the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records.

PE-10(CMS-1) – Enhancement (Moderate)

Control

Implement and maintain a master power switch or emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms.

Applicability: All	**References:** ARS: PE-10(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-10(CMS-1).1

Assessment Objective

Determine if the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms.
Interview: Organizational personnel with physical access control responsibilities to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms.
Test: Verify by physical inspection to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms.

PE-11 – Emergency Power (Moderate)

Control

Emergency power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to facilitate an orderly shutdown of the CMS information system in the event of a primary power source loss.

Guidance

Both primary and backup processing locations should be included in the safe power implementation procedures. The remote backup site's power implementation should be included in the documentation. Even though unlikely that both the primary and backup locations will be switching to emergency power at the same time, it is prudent to minimize the risk to a total lose of a processing capability.

Applicability: All	**References:** ARS: PE-11; FISCAM: TSC-2.2.5; NIST 800-53/53A: PE-11; PISP: 4.11.11	**Related Controls:**

ASSESSMENT PROCEDURE: PE-11.1

Assessment Objective

Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records.
Test: Uninterruptible power supply.(Optional)

PE-12 – Emergency Lighting (Moderate)

Control

Mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enhance safety and availability. Automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes shall be provided.

Guidance

Local building safety codes are a good place to obtain the needed information for documenting emergency lighting implementation procedures and architecture.

Applicability: All	References: ARS: PE-12; NIST 800-53/53A: PE-12; PISP: 4.11.12	Related Controls:

ASSESSMENT PROCEDURE: PE-12.1

Assessment Objective

Determine if:
(i) the organization employs and maintains automatic emergency lighting systems that activates in the event of a power outage or disruption; and
(ii) the organization employs and maintains automatic emergency lighting systems that cover emergency exits and evacuation routes.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records.
Test: Emergency lighting capability.

PE-13 – Fire Protection (Moderate)

Control

Fire protection mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to prevent, detect, and respond to fire. Fire suppression and detection devices / systems that can be activated in the event of a fire shall be employed and maintained. Fire suppression and detection devices / systems shall include, but not be limited to, sprinkler systems, hand-held fire extinguishers, fixed fire hoses, and smoke detectors.

Guidance

Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Applicability: All	References: ARS: PE-13; FISCAM: TSC-2.2.1, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-13; PISP: 4.11.13	Related Controls:

ASSESSMENT PROCEDURE: PE-13.1

Assessment Objective

Determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records.

PE-13(1) – Enhancement (Moderate)

Control

Implement and maintain fire detection devices / systems that activate automatically and notify the organization and emergency responders in the event of a fire.

Applicability: All	References: ARS: PE-13(1); NIST 800-53/53A: PE-13(1)	Related Controls:

ASSESSMENT PROCEDURE: PE-13(1).1

Assessment Objective

Determine if:
(i) the organization employs fire detection devices/systems that activate automatically; and
(ii) the organization employs fire detection devices/systems that notify the organization and emergency responders in the event of a fire.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; other relevant documents or records.
Test: Simulated fire detection and automated notifications.(Optional)

PE-13(2) – Enhancement (Moderate)		
Control Employ fire suppression devices / systems that provide automatic notification of any activation to the organization and emergency responders.		
Applicability: All	**References:** ARS: PE-13(2); NIST 800-53/53A: PE-13(2)	**Related Controls:**
ASSESSMENT PROCEDURE: PE-13(2).1		
Assessment Objective Determine if the organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders. **Assessment Methods And Objects** **Examine:** Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; other relevant documents or records. **Test:** Simulated activation of fire suppression devices/systems and automated notifications.(Optional)		
PE-13(3) – Enhancement (Moderate)		
Control Employ an automatic fire suppression capability in facilities that are not staffed on a continuous basis.		
Applicability: All	**References:** ARS: PE-13(3); NIST 800-53/53A: PE-13(3)	**Related Controls:**
ASSESSMENT PROCEDURE: PE-13(3).1		
Assessment Objective Determine if the organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis. **Assessment Methods And Objects** **Examine:** Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; other relevant documents or records. **Test:** Simulated activation of fire suppression devices/systems and automated notifications.(Optional)		
PE-14 – Temperature and Humidity Controls (Moderate)		
Control Temperature and humidity control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain (within acceptable levels) and monitor the temperature and humidity of facilities containing CMS information systems.		
Guidance Local building a safety codes are a good place to obtain the needed information for documenting HVAC implementation procedures and architecture. Consideration for Occupational Safety and Health Administration (OSHA) requirements maybe included.		
Applicability: All	**References:** ARS: PE-14; FISCAM: TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-14; PISP: 4.11.14	**Related Controls:**
ASSESSMENT PROCEDURE: PE-14.1		
Assessment Objective Determine if: (i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and (ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides. **Assessment Methods And Objects** **Examine:** Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records.		
PE-14(CMS-1) – Enhancement (Moderate)		
Control Evaluate the level of alert and follow prescribed guidelines for that alert level.		
Applicability: All	**References:** ARS: PE-14(CMS-1)	**Related Controls:**
ASSESSMENT PROCEDURE: PE-14(CMS-1).1		
Assessment Objective Determine if: (i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and		

(ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records to determine the level of alert and prescribed guidelines for that alert level.

Interview: Organizational personnel with environmental protection responsibilities to determine if there exists the level of alert and prescribed guidelines for that alert level.

PE-14(CMS-2) – Enhancement (Moderate)

Control

Alert component management of possible loss of service and/or media.

Applicability: All	**References:** ARS: PE-14(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(CMS-2).1

Assessment Objective

Determine if the organization alerts responsible management personnel of loss of service or media.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records to determine an alert is generated to component management of possible loss of service and/or media.

Interview: Organizational personnel with environmental protection responsibilities to determine an alert is generated to component management of possible loss of service and/or media

PE-14(CMS-3) – Enhancement (Moderate)

Control

Report damage and provide remedial action. Implement contingency plan, if necessary.

Applicability: All	**References:** ARS: PE-14(CMS-3)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(CMS-3).1

Assessment Objective

Determine if the organization regularly monitors the temperature and humidity within the facility where the information system resides.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records to determine damage is reported and remedial action is taken, including the implementation of contingency plan.

Interview: Organizational personnel with environmental protection responsibilities to determine to determine if damage is reported and remedial action is taken, including the implementation of contingency plan.

PE-14(FIS-1) – Enhancement (Moderate)

Control

Redundancy exists in the air cooling system.

Applicability: All	**References:** FISCAM: TSC-2.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(FIS-1).1

Assessment Objective

Determine if the organization uses redundant air cooling systems.

Assessment Methods And Objects

Examine: Entity's facilities.

Examine: Operation, location, maintenance, and access to the air cooling systems.

Examine: Pertinent policies and procedures.

Interview: Site manager.

PE-15 – Water Damage Protection (Moderate)

Control

All necessary steps shall be taken to ensure that the building plumbing does not endanger CMS information systems. Procedures shall be developed, documented, and implemented effectively to reduce the potential damage from plumbing leaks.

Guidance

Local building a safety codes are a good place to obtain the needed information for documenting water damage protection procedures and architecture. Consideration for Occupational Safety and Health Administration (OSHA) requirements maybe included.

Applicability: All	**References:** ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15; PISP: 4.11.15	**Related Controls:**

ASSESSMENT PROCEDURE: PE-15.1

Assessment Objective

Determine if:
(i) the organization identifies key personnel with knowledge of location and operational procedures for activating master shutoff valves for plumbing system; and
(ii) the organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff values; list of key personnel with knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value documentation; other relevant documents or records.
Interview: Organization personnel with physical and environmental protection responsibilities.
Test: Simulated master water shutoff value activation for the plumbing system.

PE-16 – Delivery and Removal (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to control the flow of information system-related items into and out of the organization. Appropriate officials shall authorize the delivery or removal of CMS information system-related items.

To avoid unauthorized access, delivery and removal controls shall be implemented to isolate delivery areas from sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries.

Guidance

The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.

Applicability: All	**References:** ARS: PE-16; NIST 800-53/53A: PE-16; PISP: 4.11.16	**Related Controls:**

ASSESSMENT PROCEDURE: PE-16.1

Assessment Objective

Determine if:
(i) the organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility; and
(ii) the organization maintains appropriate records of items entering and exiting the facility.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records.
Interview: Organization personnel with tracking responsibilities for information system components entering and exiting the facility.

PE-17 – Alternate Work Site (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to control information system security at alternate work sites. A method of communication shall be provided to employees at alternate work sites to report security issues or suspected security incidents.

Guidance

The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST SP 800-46 provides guidance on security in telecommuting and broadband communications.

Applicability: All	**References:** ARS: PE-17; HIPAA: 164.310(a)(2)(i); NIST 800-53/53A: PE-17; PISP: 4.11.17	**Related Controls:**

ASSESSMENT PROCEDURE: PE-17.1

Assessment Objective

Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records.

Interview: Organization personnel using alternate work sites.

PE-17(CMS-1) – Enhancement (Moderate)

Control

Employ appropriate security controls at alternate work sites. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

Applicability: All	**References:** ARS: PE-17(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-17(CMS-1).1

Assessment Objective

Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records to determine if appropriate security controls at alternate work sites are employed. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

Interview: Organizational personnel with alternate worksite responsibilities to determine if appropriate security controls at alternate work sites are employed. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

PE-18 – Location of Information System Components (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that information system components are positioned within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.

Guidance

Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Applicability: All	**References:** ARS: PE-18; FISCAM: TAN-2.1.1, TAN-2.1.2; HIPAA: 164.312(c)(1); NIST 800-53/53A: PE-18; PISP: 4.11.18	**Related Controls:**

ASSESSMENT PROCEDURE: PE-18.1

Assessment Objective

Determine if:

(i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and

(ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; other relevant documents or records.

Planning (PL) – *Management*

PL-1 – Security Planning Policy and Procedures (Moderate)

Control

All CMS information systems and major applications shall be documented in a SSP, which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, in accordance with current CMS Procedures.

Guidance

The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-18 provides guidance on security planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: PL-1; FISCAM: TSP-2.1, TSP-3.2; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2; NIST 800-53/53A: PL-1; PISP: 4.12.1	**Related Controls:**

ASSESSMENT PROCEDURE: PL-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security planning policy and procedures;
(ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review security planning policy and procedures; and
(iv) the organization updates security planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: PL-1.2

Assessment Objective

Determine if:
(i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

PL-1(FIS-1) – Enhancement (Moderate)

Control

Security policies are distributed to all affected personnel.

Applicability: All	**References:** FISCAM: TSP-3.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-1(FIS-1).1

Assessment Objective

Determine if the organization distributes security policies to all affected personnel.

Assessment Methods And Objects

Examine: Memos, electronic mail files, or other policy distribution mechanisms.
Interview: Staff and system users to determine how security policies are distributed.

PL-2 – System Security Plan (SSP) (Moderate)

Control

All CMS information systems and major applications shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18. The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization

officials and incorporated into the information resources management strategic plan. The information contained in the SSP is subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The security plan is aligned with the organization's information system architecture and information security architecture. NIST SP 800-18 provides guidance on security planning.

Applicability: All	**References:** ARS: PL-2; FISCAM: TAC-3.1.A.1, TSP-2.1, TSP-3.2; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3; NIST 800-53/53A: PL-2; PISP: 4.12.2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2.1

Assessment Objective

Determine if:
(i) the organization develops and implements a security plan for the information system;
(ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements;
(iii) the security plan development is consistent with NIST SP 800-18 and the concepts in the NIST Risk Management Framework including baseline security control selection, tailoring of the baseline, and supplementation of the tailored baseline;
(iv) the security plan is consistent with the organization's information system architecture and information security architecture; and
(v) designated organizational officials review and approve the security plan.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan development and implementation; NIST SP 800-18; security plan for the information system; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.

PL-2(CMS-1) – Enhancement (Moderate)

Control

Document the in-place security controls of the system according to the CMS System Security Plan (SSP) Procedures.

Applicability: All	**References:** ARS: PL-2(CMS-1); FISCAM: TSP-2.1; HIPAA: 164.316(b)(1)(i), 164.316(b)(1)(ii); HSPD 7: J(35); IRS-1075: 4.7.3#2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2(CMS-1).1

Assessment Objective

Determine if:
(i) the organization develops and implements a security plan for the information system;
(ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements;
(iii) the security plan is consistent with NIST SP 800-18;
(iv) the security plan is consistent with the organization's information system architecture and information security architecture; and
(v) designated organizational officials review and approve the security plan.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan development and implementation; NIST SP 800-18; security plan for the information system; other relevant documents or records to determine the in-place security controls of the system are documented according to the CMS System Security Plan (SSP) Procedures.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities to determine if System Security Plan (SSP) includes the in-place security controls of the system and are documented according to the CMS System Security Plan (SSP) Procedures.

PL-2(PII-1) – Enhancement (Moderate)

Control

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Applicability: All	**References:** HIPAA: 164.316(b)(2)(ii)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2(PII-1).1

Assessment Objective

Determine if the organization provides to those persons responsible for implementing the procedures to which the documentation pertains.

Assessment Methods And Objects

Examine: Procedures that document who obtains documentation and which documentation pertains to whom for implementation.
Interview: Organizational personnel who are responsible for implementation of procedures to determine if documentation is available.

PL-2(HIP-1) – Enhancement (Moderate)

Control

Retain documentation of policies and procedures relating to HIPAA 164.306 for 6 years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)

Applicability: All	**References:** HIPAA: 164.316(b)(2)(i)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2(HIP-1).1

Assessment Objective

Determine if the organization retains documentation of policies and procedures relating to 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b))

Assessment Methods And Objects

Examine: A sampling of documentation of policies and procedures relating to 164.306 is held for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b))

Interview: Organization personnel to determine if documentation of policies and procedures relating to 164.306 is held for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b))

PL-2(IRS-1) – Enhancement (Moderate)

Control

When FTI is incorporated into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition to those specified in other controls.

Applicability: All	**References:** IRS-1075: 5.6.3.5#3	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2(IRS-1).1

Assessment Objective

Determine if the organization incorporates FTI into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition to those specified in other controls.

Assessment Methods And Objects

Examine: Controls to determine compliance with IRS Pub 1075 Exhibit 7 while FTI is incorporated into a Data Warehouse.

PL-2(IRS-2) – Enhancement (Moderate)

Control

For FTI, develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7 & 8)

Applicability: All	**References:** IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2(IRS-2).1

Assessment Objective

Determine if the organization develops and submits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7 & 8).

Assessment Methods And Objects

Examine: Safeguard Procedure Reports to determine the procedures established and used ensure confidentially of the FTI data received from the IRS.

Examine: Safeguard Activity Reports to determine annual submission and protections are in accordance with the Safeguard Procedure Report.

PL-3 – System Security Plan Update (Moderate)

Control

The SSP shall be reviewed at least every 365 days and updated minimally every three (3) years to reflect current conditions or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security; when the data sensitivity level increases; after a serious security violation; due to changes in the threat environment; or before the previous accreditation expires.

Guidance

Significant changes are defined in advance by the organization and identified in the configuration management process. NIST SP 800-18 provides guidance on security plan updates.

Applicability: All	References: ARS: PL-3; FISCAM: TSP-2.2; HIPAA: 164.306(a)(3), 164.316(a), 164.316(b)(2)(iii); HSPD 7: G(24), J(35); IRS-1075: 5.6.1.2#1.4; NIST 800-53/53A: PL-3; PISP: 4.12.3	Related Controls:

ASSESSMENT PROCEDURE: PL-3.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of information system security plan reviews and updates;
(ii) the organization updates the security plan in accordance with organization-defined frequency, at least annually;
(iii) the organization receives input to update the security plan from the organization's configuration management and control process; and
(iv) the updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan updates; information system security plan; configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records.

PL-4 – Rules of Behavior (ROB) (Moderate)

Control

ROBs shall be established, and made readily available, to delineate clearly user responsibilities and expected behavior of all Business Owners, users, operators, and administrators with regard to information and information system usage. Before authorizing access to the information system and / or information and annually thereafter, the organization shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the ROBs. Specific ROBs shall be established to govern work-at-home users who access CMS information or information systems.

Limited personal use of organization-owned or leased equipment and resources shall be considered to be a permitted use of organization-owned or leased equipment and resources when the following conditions are met:
4.12.4.1. Such use involves minimal additional expense to CMS;
4.12.4.2. Such use does not interfere with the mission or operation of CMS;
4.12.4.3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch;
4.12.4.4. Such use does not overburden any CMS information system resources;
4.12.4.5. Such use is not otherwise prohibited under this policy; and
4.12.4.6. Any use of organizational Internet and email resources shall be made with the understanding that such use is not secure, private or anonymous.

The following uses of organization-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited:
4.12.4.7. Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace;
4.12.4.8. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords;
4.12.4.9. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity;
4.12.4.10. All email communications to groups of employees that are subject to approval prior to distribution and have not been approved by the organization (e.g., retirement announcements, union notices or announcements, charitable solicitations); and
4.12.4.11. Employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees.

All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of organization-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that employees desire to protect their privacy, employees shall not use organization-owned or leased equipment and resources.

Guidance

Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST SP 800-18 provides guidance on preparing rules of behavior.

Applicability: All	References: ARS: PL-4; FISCAM: TSP-3.3.2; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.5; NIST 800-53/53A: PL-4; PISP: 4.12.4	Related Controls:

ASSESSMENT PROCEDURE: PL-4.1

Assessment Objective

Determine if:
(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;
(ii) the organization makes the rules available to all information system users;
(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and

(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records.

Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior.

PL-4(CMS-1) – Enhancement (Moderate)

Control

Define user roles and expectations for system and network use.

Applicability: All	**References:** ARS: PL-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-4(CMS-1).1

Assessment Objective

Determine if:

(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;

(ii) the organization makes the rules available to all information system users;

(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and

(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records to determine user roles and expectations for system and network use are defined.

Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior to determine user roles and expectations for system and network use are defined.

PL-4(CMS-2) – Enhancement (Moderate)

Control

Electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

Applicability: All	**References:** ARS: PL-4(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-4(CMS-2).1

Assessment Objective

Determine if:

(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;

(ii) the organization makes the rules available to all information system users;

(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and

(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records to determine electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior to determine electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

PL-5 – Privacy Impact Assessment (PIA) (Moderate)

Control

PIAs shall be conducted for CMS information systems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandum M-03-22, and the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations.

Guidance

OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

Applicability: All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC,	**References:** ARS: PL-5; HSPD 7: J(35); NIST 800-53/53A: PL-5; PISP: 4.12.5	**Related Controls:**

SS, ZPIC		
ASSESSMENT PROCEDURE: PL-5.1		
Assessment Objective Determine if: (i) the organization conducts a privacy impact assessment on the information system in accordance with OMB policy; and (ii) the privacy impact assessment is consistent with federal legislation and OMB policy. **Assessment Methods And Objects** **Examine:** Security planning policy; procedures addressing privacy impact assessments on the information system; appropriate federal legislation and OMB policy; privacy impact assessment; other relevant documents or records.		
PL-6 – Security-Related Activity Planning (Moderate)		
Control Security-related activities affecting the information system shall be planned and coordinated before being performed in order to reduce the impact on CMS operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing / exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.		
Guidance Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.		
Applicability: All	**References:** ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6	**Related Controls:**
ASSESSMENT PROCEDURE: PL-6.1		
Assessment Objective Determine if: (i) the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations, organizational assets, and individuals; and (ii) the organization's advance planning and coordination of security-related activities includes both emergency and non-emergency situations. **Assessment Methods And Objects** **Examine:** Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records. **Interview:** Organizational personnel with information system security planning and plan implementation responsibilities.		

Personnel Security (PS) – *Operational*

PS-1 – Personnel Security Policy and Procedures (Moderate)		
Control CMS information systems shall employ personnel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines. Procedures shall be developed to guide the implementation of personnel security controls.		
Guidance The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.		
Applicability: All	**References:** ARS: PS-1; FISCAM: TSD-1.3.3; IRS-1075: 5.6.2.1#1.1-2; NIST 800-53/53A: PS-1; PISP: 4.13.1	**Related Controls:**
ASSESSMENT PROCEDURE: PS-1.1		
Assessment Objective Determine if: (i) the organization develops and documents personnel security policy and procedures; (ii) the organization disseminates personnel security policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review personnel security policy and procedures; and (iv) the organization updates personnel security policy and procedures when organizational review indicates updates are required. **Assessment Methods And Objects** **Examine:** Personnel security policy and procedures, other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.(Optional)		
ASSESSMENT PROCEDURE: PS-1.2		
Assessment Objective Determine if: (i) the personnel security policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the personnel security policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the personnel security procedures address all areas identified in the personnel security policy and address achieving policy-compliant implementations of all associated security controls. **Assessment Methods And Objects** **Examine:** Personnel security policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.(Optional)		
PS-1(FIS-1) – Enhancement (Moderate)		
Control Staff's performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.		
Applicability: All	**References:** FISCAM: TSD-2.2.1	**Related Controls:**
ASSESSMENT PROCEDURE: PS-1(FIS-1).1		
Assessment Objective Determine if the organization monitors staff performance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are carried out. **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes). **Interview:** Management and subordinate personnel.		
PS-1(FIS-2) – Enhancement (Moderate)		
Control Regularly scheduled vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.		
Applicability: All	**References:** FISCAM: TSD-1.1.7, TSP-4.1.4, TSP-4.1.5	**Related Controls:**

ASSESSMENT PROCEDURE: PS-1(FIS-2).1

Assessment Objective

Determine if the organization regularly schedules vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.

Assessment Methods And Objects

Examine: Personnel records to identify individuals who have not taken vacation or sick leave in the past year.
Examine: Staff assignment records and determine whether job and shift rotations occur.
Examine: Vacation and job rotation policies and procedures.
Interview: Information system management and users.

PS-1(FIS-3) – Enhancement (Moderate)

Control

Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes. Employees are made aware of their job descriptions.

Applicability: All	**References:** FISCAM: TSD-1.2.2, TSD-1.3.1, TSP-4.2.1, TSS-2.1.2, TSS-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: PS-1(FIS-3).1

Assessment Objective

Determine if:
(i) the organizational documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes.
(ii) the organization makes the employees aware of their job descriptions.

Assessment Methods And Objects

Examine: Effective dates of the position descriptions and determine whether they are current.
Examine: Job descriptions for several positions in organizational units and for user security administrators.
Examine: Job descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
Interview: Management personnel.

PS-2 – Position Categorization (Moderate)

Control

A criticality / sensitivity rating (e.g., non-sensitive, national security, public trust) shall be assigned to all positions within the organization. The criticality / sensitivity rating shall be in compliance with 5 CFR 731.106(a), Executive Orders 10450 and 12968, NSPD-1, HSPD-7, and HSPD-12 and consistent with OPM policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating. All criticality / sensitivity ratings must be submitted to the DHHS HR department and CMS' personnel security department.

Guidance

Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Applicability: All	**References:** ARS: PS-2; IRS-1075: 5.6.2.1#1.3; NIST 800-53/53A: PS-2; PISP: 4.13.2	**Related Controls:**

ASSESSMENT PROCEDURE: PS-2.1

Assessment Objective

Determine if:
(i) the organization assigns a risk designations to all positions within the organization;
(ii) the organization establishes a screening criteria for individuals filling organizational positions;
(iii) the risk designations for the organizational positions are consistent with applicable federal regulations and OPM policy and guidance;
(iv) the organization defines the frequency of risk designation reviews and updates for organizational positions; and
(v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan; records of risk designation reviews and updates; other relevant documents or records.

PS-2(0) – Enhancement (Moderate)

Control

Review and revise position risk designations every 365 days.

Applicability: All	References: ARS: PS-2(0); NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:

ASSESSMENT PROCEDURE: PS-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan (for organization-defined frequency for review of position categorizations); records of risk designation reviews and updates; other relevant documents or records.

PS-3 – Personnel Screening (Moderate)

Control

Prior to being granted access, all employees and contractors who require access to CMS information or information systems shall be screened and reinvestigated periodically, consistent with the criticality / sensitivity rating of the position. For prospective employees, references background checks shall be performed before issuance of a User ID. Security agreements shall be required for employees and contractors assigned to work with mission critical information.

Guidance

Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and SP 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.

Applicability: All	References: ARS: PS-3; FISCAM: TSP-4.1.1, TSP-4.1.2; IRS-1075: 5.6.2.1#1.4; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:

ASSESSMENT PROCEDURE: PS-3.1

Assessment Objective

Determine if:

(i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and

(ii) the personnel screening is consistent with appropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 800-78; other relevant documents or records.

PS-3(0) – Enhancement (Moderate)

Control

Perform criminal history check for all persons prior to employment.

Applicability: All	References: ARS: PS-3(0); FISCAM: TSP-4.1.2; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:

ASSESSMENT PROCEDURE: PS-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 800-78; other relevant documents or records.

PS-3(CMS-1) – Enhancement (Moderate)

Control

Require personnel to obtain and hold a moderate-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook.

Applicability: All	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:

ASSESSMENT PROCEDURE: PS-3(CMS-1).1

Assessment Objective

Determine if:

(i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and

(ii) the personnel screening is consistent with appropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; and other relevant documents or records to determine that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.
Interview: Personnel with personnel screening responsibilities to confirm that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

PS-4 – Personnel Termination (Moderate)

Control

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information and information systems is removed upon personnel termination. Termination procedures shall address:
4.13.4.1. Exit interviews;
4.13.4.2. Retrieval of all organizational information system-related property;
4.13.4.3. Notification to security management;
4.13.4.4. Revocation of all system access privileges;
4.13.4.5. Immediately escorting employees terminated for cause out of organization facilities; and
4.13.4.6. Hard disk back up and sanitization before re-issuance.

Appropriate personnel shall have access to official records created by the terminated employee that are stored on organizational information systems.

Guidance

Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Applicability: All	**References:** ARS: PS-4; FISCAM: TAC-2.1.6, TSP-4.1.6; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: 5.6.2.1#1.5; NIST 800-53/53A: PS-4; PISP: 4.13.4	**Related Controls:**

ASSESSMENT PROCEDURE: PS-4.1

Assessment Objective

Determine if:
(i) the organization terminates information system access upon termination of individual employment;
(ii) the organization conducts exit interviews of terminated personnel;
(iii) the organization retrieves all organizational information system-related property from terminated personnel; and
(iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities.

PS-4(CMS-1) – Enhancement (Moderate)

Control

Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

Applicability: All	**References:** ARS: PS-4(CMS-1); FISCAM: TAC-3.2.C.4	**Related Controls:**

ASSESSMENT PROCEDURE: PS-4(CMS-1).1

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.
Interview: Personnel with termination responsibilities to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

PS-5 – Personnel Transfer (Moderate)

Control

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information or information systems no longer required in the new assignment is

terminated upon personnel transfer. Transfer procedures shall address:

4.13.5.1. Re-issuing appropriate organizational information system-related property (e.g., keys, identification cards, building passes);
4.13.5.2. Notification to security management;
4.13.5.3. Closing obsolete accounts and establishing new accounts; and
4.13.5.4. Revocation of all system access privileges (if applicable).

Guidance

Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts.

Applicability: All	**References:** ARS: PS-5; FISCAM: TAC-2.1.6, TSP-4.1.6; IRS-1075: 5.6.2.1#1.6; NIST 800-53/53A: PS-5; PISP: 4.13.5	**Related Controls:**

ASSESSMENT PROCEDURE: PS-5.1

Assessment Objective

Determine if:
(i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and
(ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

PS-6 – Access Agreements (Moderate)

Control

Individuals who require access to CMS information or information systems shall be required to complete and sign appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements.

Guidance

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Applicability: All	**References:** ARS: PS-6; FISCAM: TSP-4.1.3; IRS-1075: 5.6.2.1#1.7; NIST 800-53/53A: PS-6; PISP: 4.13.6	**Related Controls:**

ASSESSMENT PROCEDURE: PS-6.1

Assessment Objective

Determine if:
(i) the organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access;
(ii) organizational personnel sign access agreements;
(iii) the organization defines the frequency of reviews and updates for access agreements; and
(iv) the organization reviews and updates the access agreements in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records.

PS-6(0) – Enhancement (Moderate)

Control

Access agreements are reviewed and updated as part of the system accreditation or when a contract is renewed or extended.

Applicability: All	**References:** ARS: PS-6(0); NIST 800-53/53A: PS-6; PISP: 4.13.6	**Related Controls:**

ASSESSMENT PROCEDURE: PS-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan (for organization-defined

frequency for access agreement reviews); access agreements; records of access agreement reviews and updates; other relevant documents or records.

PS-7 – Third-Party Personnel Security (Moderate)

Control

Personnel security controls employed by external service providers and third parties shall be documented, agreed to, implemented effectively, and monitored for compliance and shall include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements. Personnel security controls employed by service providers and third parties shall be compliant with CMS IS policies and procedures, and consistent with NIST SP 800-35.

Guidance

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST SP 800-35 provides guidance on information technology security services.

Applicability: All	**References:** ARS: PS-7; IRS-1075: 5.6.2.1#1.8; NIST 800-53/53A: PS-7; PISP: 4.13.7	**Related Controls:**

ASSESSMENT PROCEDURE: PS-7.1

Assessment Objective

Determine if:
(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management);
(ii) the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST SP 800-35; and
(iii) the organization monitors third-party provider compliance with personnel security requirements.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities; third-party providers.

PS-7(CMS-1) – Enhancement (Moderate)

Control

Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.

Applicability: All	**References:** ARS: PS-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PS-7(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management); and
(ii) the organization monitors third-party provider compliance with personnel security requirements.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records to determine the access provided to contractors and defining security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.
Interview: Personnel with third party security responsibilities to determine that the access provided to contractors are defined within the security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.

PS-8 – Personnel Sanctions (Moderate)

Control

The organization shall enforce formal personnel sanctions process for personnel who fail to comply with established CMS IS policies and procedures. The employee sanction process shall be consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines.

Guidance

The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Applicability: All	References: ARS: PS-8; HIPAA: 164.308(a)(1)(ii)(C); NIST 800-53/53A: PS-8; PISP: 4.13.8	Related Controls:

ASSESSMENT PROCEDURE: PS-8.1

Assessment Objective

Determine if:
(i) the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
(ii) the personnel sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records.

PS-CMS-1 – Review System Access during Extraordinary Personnel Circumstances (Moderate)

Control

Access to CMS information and information systems shall be reviewed during extraordinary personnel circumstances and limited as deemed necessary.

Guidance

A death in the family or other personal problems could be considered extraordinary personal circumstances. For some personnel, recovery from a difficult time may take longer than usual and management must consider the circumstances on a case by case basis.

Applicability: All	References: ARS: PS-9; PISP: 4.13.9	Related Controls:

ASSESSMENT PROCEDURE: PS-CMS-1.1

Assessment Objective

Determine if the organization manages personnel with extraordinary personal circumstances.

Assessment Methods And Objects

Examine: Personnel security policy and procedures; other relevant documents or records determine system access during extraordinary personnel circumstances is reviewed and access is limited as deemed necessary.

Interview: Organizational personnel with personnel security responsibilities to determine system access during extraordinary personnel circumstances is reviewed and access is limited as deemed necessary.

PS-CMS-2 – Designate an Information System Security Officer (ISSO) / System Security Officer (SSO) (Moderate)

Control

An Information System Security Officer (ISSO) / System Security Officer (SSO) shall be designated for each business component with roles and responsibilities of the position clearly defined.

Guidance

A good reference set for defining the Information System Security Officer (ISSO) / System Security Officer (SSO) responsibilities are the NIST SPs. Specific responsibilities should be developed to protect CMS information systems and data.

Applicability: All	References: ARS: PS-10; FISCAM: TSP-3.1.1, TSP-3.1.2; HIPAA: 164.308(a)(2); PISP: 4.13.10	Related Controls:

ASSESSMENT PROCEDURE: PS-CMS-2.1

Assessment Objective

Determine if the organization has documented the roles and responsibilities of appointed ISSO / SSO.

Assessment Methods And Objects

Examine: Personnel security policy and procedures; other relevant documents or records to determine an ISSO / SSO is designated for each component with roles and responsibilities of the position clearly defined.

Interview: Organizational personnel with personnel security responsibilities to determine an ISSO / SSO is designated for each component with roles and responsibilities of the position clearly defined.

Risk Assessment (RA) – *Management*

RA-1 – Risk Assessment Policy and Procedures (Moderate)

Control

All CMS applications and systems shall be covered by an IS RA. The RA shall be consistent with NIST SP 800-30. Formal documented procedures shall be developed, disseminated, and reviewed / updated periodically to facilitate the implementation of the RA policy and associated RA controls. The procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-30 provides guidance on the assessment of risk. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: RA-1; FISCAM: TAC-3.1.A.2; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075: 5.6.1.1#1.1-2; NIST 800-53/53A: RA-1; PISP: 4.14.1	**Related Controls:**

ASSESSMENT PROCEDURE: RA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents risk assessment policy and procedures;
(ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review risk assessment policy and procedures; and
(iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.(Optional)

ASSESSMENT PROCEDURE: RA-1.2

Assessment Objective

Determine if:
(i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.(Optional)

RA-2 – Security Categorization (Moderate)

Control

CMS information systems and the information processed, stored, or transmitted by the systems shall be categorized in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to the, CMS System Security Level by Information Type. The security categorization (including supporting rationale) shall be explicitly documented. Designated senior-level officials within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the CMS CIO, CISO, and Business Owners.

All CMS information systems categorized as high or moderate shall be considered sensitive or to contain sensitive information. All CMS information systems categorized as low shall be considered non-sensitive or to contain non-sensitive information. All CMS information systems shall implement minimum security requirements and controls as established in the current CMS IS Standards, based on security categorization of the system.

Guidance

The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST SP 800-60 provides guidance on determining the security categories of the

information types resident on the information system.

Applicability: All	**References:** ARS: RA-2; FISCAM: TAC-1.1; HSPD 7: D(8); IRS-1075: 4.1#2; NIST 800-53/53A: RA-2; PISP: 4.14.2	**Related Controls:** MP-4, SC-7

ASSESSMENT PROCEDURE: RA-2.1

Assessment Objective

Determine if:

(i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners;

(ii) the security categorization is consistent with FIPS 199 and NIST SP 800-60;

(iii) the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts;

(iv) the organization includes supporting rationale for impact-level decisions as part of the security categorization; and

(v) designated, senior-level organizational officials review and approve the security categorization of the information system.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST SP 800-60; information system security plan; other relevant documents or records.

Interview: Organizational personnel with security categorization and risk assessment responsibilities.

RA-3 – Risk Assessment (RA) (Moderate)

Control

An assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that support the operations and assets of CMS shall be performed, both within CMS and by external parties that manage / operate information or information systems for CMS. The RA shall be in accordance with current CMS Procedures. Based on the operation of the information system, the RA shall take into account vulnerabilities, threat sources, and security controls in place to determine the resulting level of residual risk posed to CMS operations, CMS assets, CMS information, or individuals.

Any findings from reviews of CMS systems shall be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses shall be documented by the Business Owner or external party and addressed by mitigating the risk, accepting the risk with explanation or submitting Corrective Action Plan (CAP). These findings shall be subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST SP 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Applicability: All	**References:** ARS: RA-3; FISCAM: TAC-3.1.A.2, TSP-1.1.2, TSP-1.1.3, TSP-5.1.4; HIPAA: 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3, 6.3.3#2; NIST 800-53/53A: RA-3; PISP: 4.14.3	**Related Controls:**

ASSESSMENT PROCEDURE: RA-3.1

Assessment Objective

Determine if:

(i) the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and

(ii) the risk assessment is consistent with the NIST SP 800-30.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST SP 800-30; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

RA-3(CMS-1) – Enhancement (Moderate)

Control

Perform an IS RA for the system, and document the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

Applicability: All	**References:** ARS: RA-3(CMS-1); FISCAM: TAC-1.1, TAC-1.2, TSS-2.2.4; HIPAA: 164.306(a)(2); HSPD 7: D(8), F(19)	**Related Controls:**

ASSESSMENT PROCEDURE: RA-3(CMS-1).1

Assessment Objective

Determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties).

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; information system security plan (for organization-defined frequency for risk assessment updates); records of risk assessment updates; NIST SP 800-30; other relevant documents or records to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

Interview: Organizational personnel with risk assessment responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

RA-4 – Risk Assessment Update (Moderate)

Control

The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation.

Guidance

The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates.

Applicability: All	**References:** ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4	**Related Controls:**

ASSESSMENT PROCEDURE: RA-4.1

Assessment Objective

Determine if:

(i) the organization defines the frequency of risk assessment updates;

(ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system;

(iii) the risk assessment update is consistent with the NIST SP 800-30; and

(iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing risk assessment updates; risk assessment; information system security plan; records of risk assessment updates; NIST SP 800-30; other relevant documents or records.

RA-5 – Vulnerability Scanning (Moderate)

Control

Appropriate vulnerability assessment tools and techniques shall be implemented by the organization. Selected personnel shall be trained in their use and maintenance. The organization shall conduct periodic testing of its security posture by scanning its information systems with vulnerability tools. The information obtained from the vulnerability scanning process shall be shared with appropriate personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems. The activities of employees using organization Internet and email resources shall be subject to monitoring by system or security personnel without notice.

Guidance

Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST SP 800-42 provides guidance on

network security testing. NIST SP 800-40 (Version 2) provides guidance on patch and vulnerability management.

Applicability: All	References: ARS: RA-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5; PISP: 4.14.5	Related Controls:

ASSESSMENT PROCEDURE: RA-5.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of vulnerability scans within the information system;
(ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported;
(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact;
(iv) the organization performs network vulnerability scanning in accordance with NIST SP 800-42; and
(v) the organization handles patch and vulnerability management in accordance with NIST SP 800-40.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.(Optional)

RA-5(0) – Enhancement (Moderate)

Control

Utilize appropriate vulnerability scanning tools and techniques to scan for vulnerabilities in the information system every 90 days or when significant new vulnerabilities are identified and reported.

Applicability: All	References: ARS: RA-5(0); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5; PISP: 4.14.5	Related Controls:

ASSESSMENT PROCEDURE: RA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for vulnerability scanning); vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.(Optional)

RA-5(CMS-1) – Enhancement (Moderate)

Control

Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once a year, in accordance with CMS IS procedures. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.

Applicability: All	References: ARS: RA-5(CMS-1); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24)	Related Controls:

ASSESSMENT PROCEDURE: RA-5(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines the frequency of vulnerability scans within the information system;
(ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported; and
(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for vulnerability scanning); vulnerability scanning results; patch and vulnerability management records; other relevant documents or records to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE)

naming convention.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE) naming convention.

System and Services Acquisition (SA) – *Management*

SA-1 – System and Services Acquisition Policy and Procedures (Moderate)

Control

Documented procedures shall be developed and implemented effectively to facilitate the implementation of the system and services acquisition security controls in all system and services acquisitions. Procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and services acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: SA-1; IRS-1075: 5.6.1.3#1.1-2; NIST 800-53/53A: SA-1; PISP: 4.15.1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and services acquisition policy and procedures;
(ii) the organization disseminates system and services acquisition policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and services acquisition policy and procedures; and
(iv) the organization updates system and services acquisition policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)

ASSESSMENT PROCEDURE: SA-1.2

Assessment Objective

Determine if:
(i) the system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and services acquisition policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and services acquisition procedures address all areas identified in the system and services acquisition policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)

SA-1(IRS-1) – Enhancement (Moderate)

Control

For FTI, develop, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes IRS documents received and identified by:
(a) taxpayer name
(b) tax year(s)
(c) type of information (e.g., revenue agent reports, Form 1040, work papers)
(d) the reason for the request
(e) date requested
(f) date received
(g) exact location of the FTI
(h) who has had access to the data and
(i) if disposed of, the date and method of disposition.

Applicability: All	**References:** IRS-1075: 3.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-1(IRS-1).1

Assessment Objective

Determine if the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes IRS documents received and identified by:

(a) taxpayer name
(b) tax year(s)
(c) type of information (e.g., revenue agent reports, Form 1040, work papers)
(d) the reason for the request
(e) date requested
(f) date received
(g) exact location of the FTI
(h) who has had access to the data and
(i) if disposed of, the date and method of disposition.

Assessment Methods And Objects

Examine: Organizational documentation that contains the development, dissemination and review/updates to FTI IRS documents received that show:
(a) taxpayer name
(b) tax year(s)
(c) type of information (e.g., revenue agent reports, Form 1040, work papers)
(d) the reason for the request
(e) date requested
(f) date received
(g) exact location of the FTI
(h) who has had access to the data and
(i) if disposed of, the date and method of disposition.

SA-2 – Allocation of Resources (Moderate)

Control

As part of the capital planning and investment control processes, CMS or the external organization shall determine, document, and allocate the resources required to protect CMS information systems adequately. IS requirements shall be included in mission / business case planning, and a separate line item shall be established in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Guidance

The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST SP 800-65 provides guidance on integrating security into the capital planning and investment control process.

Applicability: All	**References:** ARS: SA-2; NIST 800-53/53A: SA-2; PISP: 4.15.2	**Related Controls:**

ASSESSMENT PROCEDURE: SA-2.1

Assessment Objective

Determine if:
(i) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system;
(ii) the organization determines security requirements for the information system in mission/business case planning;
(iii) the organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation; and
(iv) the organization's programming and budgeting process is consistent with NIST SP 800-65.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST SP 800-65; other relevant documents or records.
Interview: Organizational personnel with capital planning and investment responsibilities.(Optional)

SA-3 – Life Cycle Support (Moderate)

Control

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

Guidance

NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Applicability: All	**References:** ARS: SA-3; FISCAM: TAY-1.2.1, TCC-1.1.2; NIST 800-53/53A: SA-3; PISP: 4.15.3	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3.1

Assessment Objective

Determine if:
(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and

(ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation; other relevant documents or records.

Interview: Organizational personnel with information security and system life cycle development responsibilities.(Optional)

SA-3(CMS-1) – Enhancement (Moderate)

Control

Must comply with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

Applicability: All	**References:** ARS: SA-3(CMS-1); FISCAM: TCC-1.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3(CMS-1).1

Assessment Objective

Determine if:

(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and

(ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation; other relevant documents or records to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

Interview: Organizational personnel with information security and system life cycle development responsibilities to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

SA-3(FIS-1) – Enhancement (Moderate)

Control

Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.

Applicability: All	**References:** FISCAM: TCC-2.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3(FIS-1).1

Assessment Objective

Determine if the organizational detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.

Assessment Methods And Objects

Examine: Design system specifications.

Examine: Pertinent policies and procedures.

Interview: Programmer and programming supervisor.

SA-4 – Acquisitions (Moderate)

Control

Security requirements and/or security specifications shall be included, either explicitly or by reference, in all information system acquisition contracts based on an assessment of risk in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

Solicitation Documents

Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required:

4.15.4.1. Security capabilities;

4.15.4.2. Design and development processes;

4.15.4.3. Test and evaluation procedures; and

4.15.4.4. Documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats / vulnerabilities are identified and as new technologies are implemented

Use of Evaluated and Validated Products

For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources:

1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

Configuration Settings and Implementation Guidance
The information system required documentation shall include security configuration settings, including documentation explaining exceptions to the standard, and security implementation guidance.

Guidance

Solicitation Documents
The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST SP 800-36 provides guidance on the selection of information security products. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Information System Documentation
The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

Use of Tested, Evaluated, and Validated Products
NIST SP 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.

Configuration Settings and Implementation Guidance
The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on configuration settings for information technology products.

Applicability: All	**References:** ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4	**Related Controls:**

ASSESSMENT PROCEDURE: SA-4.1

Assessment Objective

Determine if:
(i) the organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards;
(ii) the organization's acquisition of commercial information technology products is consistent with NIST SP 800-23;
(iii) references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST SP 800-70; and
(iv) acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe:
- required security capabilities;
- required design and development processes;
- required test and evaluation procedures; and
- required documentation.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.
Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.(Optional)

SA-4(1) – Enhancement (Moderate)

Control

Ensure solicitation documents require that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Applicability: All	**References:** ARS: SA-4(1); NIST 800-53/53A: SA-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-4(1).1

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.

SA-4(CMS-1) – Enhancement (Moderate)

Control

Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

Applicability: All	**References:** ARS: SA-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-4(CMS-1).1

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records to determine that all contracts and Statements of Work (SOW) that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities to determine that all contracts and SOW that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

SA-5 – Information System Documentation (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

Guidance

Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Applicability: All	**References:** ARS: SA-5; FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1, TSD-3.1.2, TSD-3.1.3, TSP-3.3.2; IRS-1075: 5.6.1.3#1.3; NIST 800-53/53A: SA-5; PISP: 4.15.5	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5.1

Assessment Objective

Determine if:

(i) the organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system;

(ii) the organization makes available information on configuring, installing, and operating the information system; and

(iii) the organization makes available information on effectively using the security features in the information system.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; other relevant documents or records.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.(Optional)

SA-5(1) – Enhancement (Moderate)		
Control Ensure that system documentation describes the functional properties of the security controls implemented within the information system with sufficient detail to facilitate analysis and testing of the controls.		
Applicability: All	**References:** ARS: SA-5(1); NIST 800-53/53A: SA-5(1)	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(1).1		
Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records. **Interview:** Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system.		
SA-5(CMS-1) – Enhancement (Moderate)		
Control Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.		
Applicability: All	**References:** ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(CMS-1).1		
Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance; and required personnel training to include administrators and users. **Interview:** Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance; and required personnel training to include administrators and users.		
SA-5(CMS-2) – Enhancement (Moderate)		
Control Maintain an updated list of related system operations and security documentation.		
Applicability: All	**References:** ARS: SA-5(CMS-2); FISCAM: TSD-1.1.6	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(CMS-2).1		
Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization maintains an updated list of related system's operations and security documentation. **Interview:** Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization maintains an updated list of related system's operations and security documentation.		
SA-5(CMS-3) – Enhancement (Moderate)		
Control Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.		
Applicability: All	**References:** ARS: SA-5(CMS-3); FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(CMS-3).1

Assessment Objective

Determine if responsible parties within the organization periodically review system and services acquisition policy and procedures.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization updates documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine if the organization updates documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.

SA-5(CMS-4) – Enhancement (Moderate)

Control

Document the system's configuration, and procedures in support of system access administration and operations.

Applicability: All	**References:** ARS: SA-5(CMS-4); FISCAM: TSD-1.1.6	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(CMS-4).1

Assessment Objective

Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization documents the system's configuration and procedures in support of system access administration and operations.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization documents the system's configuration and procedures in support of system access administration and operations.

SA-5(FIS-1) – Enhancement (Moderate)

Control

Goals are established by senior management on the availability of data processing and on-line services. Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.

Applicability: All	**References:** FISCAM: TSC-2.4.6, TSC-2.4.9	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(FIS-1).1

Assessment Objective

Determine if the organizational goals are established by senior management on the availability of data processing and on-line services. Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation.

Interview: Senior management, data processing management, and user management.

SA-5(FIS-2) – Enhancement (Moderate)

Control

Records are maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.

Applicability: All	**References:** FISCAM: TSC-2.4.7, TSC-2.4.8	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5(FIS-2).1

Assessment Objective

Determine if the organizational records are maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation.
Interview: Senior management, data processing management, and user management.

SA-6 – Software Usage Restrictions (Moderate)

Control

All software or shareware and associated documentation used on CMS information systems shall be deployed and maintained in accordance with appropriate license agreements and copyright laws. Software associated documentation protected by quantity licenses shall be managed through a tracking system to control copying and distribution. All other uses not specifically authorized by the license agreement shall be prohibited. The use of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Guidance

Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Applicability: All	**References:** ARS: SA-6; FISCAM: TCC-2.3.1; IRS-1075: 4.7.3#1.2; NIST 800-53/53A: SA-6; PISP: 4.15.6	**Related Controls:**

ASSESSMENT PROCEDURE: SA-6.1

Assessment Objective

Determine if:
(i) the organization complies with software usage restrictions; and
(ii) the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records.
Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.(Optional)

SA-6(FIS-1) – Enhancement (Moderate)

Control

Implementation orders, including effective date, are provided to all locations where they are maintained on file.

Applicability: All	**References:** FISCAM: TCC-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: SA-6(FIS-1).1

Assessment Objective

Determine if the organization provides to all locations software implementation orders, including effective date, where the orders are maintained on file.

Assessment Methods And Objects

Examine: Implementation orders.
Examine: Pertinent policies and procedures.
Interview: Information system and security administrators.

SA-7 – User Installed Software (Moderate)

Control

All users shall be restricted from downloading or installing software, unless explicitly authorized in writing by the CIO or his/her designated representative. Users that have been granted such authorization may download and install only organization-approved software. The use of install-on-demand software shall be restricted.

Guidance

If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Applicability: All	**References:** ARS: SA-7; FISCAM: TCC-1.3.1; NIST 800-53/53A: SA-7; PISP: 4.15.7	**Related Controls:**

ASSESSMENT PROCEDURE: SA-7.1

Assessment Objective

Determine if:

(i) the organization enforces explicit rules governing the installation of software by users;
(ii) unauthorized software is present on the system; and
(iii) the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary action.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records.
Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.
Test: Enforcement of rules for user installed software on the information system; information system for prohibited software.(Optional)

SA-7(CMS-1) – Enhancement (Moderate)

Control

If user installed software is authorized in writing by the CIO or his/her designated representative, ensure that business rules and technical controls enforce the documented authorizations and prohibitions.

Applicability: All	**References:** ARS: SA-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-7(CMS-1).1

Assessment Objective

Determine if:
(i) the organization enforces explicit rules governing the installation of software by users; and
(ii) unauthorized software is present on the system.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records to determine that policies exist that ensure business rules and technical controls enforce the documented authorizations and prohibitions.
Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine that policies exist that ensure business rules and technical controls enforce the documented authorizations and prohibitions.
Test: Enforcement of rules for user installed software on the information system; information system for prohibited software to determine authorizations and prohibitions.

SA-8 – Security Engineering Principles (Moderate)

Control

CMS information systems shall be designed and implemented using accepted security engineering principles.

Guidance

NIST SP 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

Applicability: All	**References:** ARS: SA-8; FISCAM: TAY-2.1.1, TAY-2.2.1, TCC-2.1.3; NIST 800-53/53A: SA-8; PISP: 4.15.8	**Related Controls:**

ASSESSMENT PROCEDURE: SA-8.1

Assessment Objective

Determine if:
(i) the organization designs and implements the information system using security engineering principles; and
(ii) the organization considers security design principles in the development and implementation of the information system consistent with NIST SP 800-27.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST SP 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)

SA-8(0) – Enhancement (Moderate)

Control

Design and implement the information system using the security engineering principles detailed in NIST SP 800-27 Rev. A, Engineering Principles for IT Security (A Baseline for Achieving Security).

Applicability: All	**References:** ARS: SA-8(0); FISCAM: TCC-2.1.3; NIST 800-53/53A: SA-8; PISP: 4.15.8	**Related Controls:**

ASSESSMENT PROCEDURE: SA-8(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST SP 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)

SA-9 – External Information System Services (Moderate)

Control

All external information system services shall include specific provisions requiring the service provider to comply with CMS IS policies, standards, and guidelines; and shall be monitored for compliance. CMS shall define the remedies for any loss, disruption, or damage caused by the service provider's failure to comply. Service providers shall be prohibited from outsourcing any system function overseas, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representatives with concurrence from CMS' personnel security department.

Guidance

An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on the security considerations in the system development life cycle.

Applicability: All	**References:** ARS: SA-9; FISCAM: TAY-1.3.1; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4; NIST 800-53/53A: SA-9; PISP: 4.15.9	**Related Controls:** CA-3

ASSESSMENT PROCEDURE: SA-9.1

Assessment Objective

Determine if:

(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;

(ii) the organization monitors security control compliance;

(iii) the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions; and

(iv) the security controls employed by providers of external information system services are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.(Optional)

SA-9(CMS-1) – Enhancement (Moderate)

Control

If service providers are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas, ensure that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Applicability: All	**References:** ARS: SA-9(CMS-1); HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-9(CMS-1).1

Assessment Objective

Determine if the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

SA-9(HIP-1) – Enhancement (Moderate)

Control

A covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a).)

Applicability: All	References: HIPAA: 164.308(b)(1), 164.308(b)(4), 164.314(a)(1)(i), 164.314(a)(2)(i), 164.314(a)(2)(i)(A), 164.314(a)(2)(i)(B), 164.314(a)(2)(i)(C), 164.314(a)(2)(i)(D), 164.314(a)(2)(ii)(A)(1), 164.314(a)(2)(ii)(A)(2), 164.314(a)(2)(ii)(B)	Related Controls:

ASSESSMENT PROCEDURE: SA-9(HIP-1).1

Assessment Objective

Determine if the organizational covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a))

Assessment Methods And Objects

Examine: Organizational documentation meets the requirements set forth in HIPAA regulations (See HIPAA 164.308(b) and 164.314(a)) for a covered entity.

Interview: Organizational personnel maintaining covered entity documentation follow requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a).)

SA-10 – Developer Configuration Management (Moderate)

Control

Information system developers shall develop, document, and implement a configuration management plan for each information system under development. The configuration management plan shall address change control mechanisms during development, change authorization requirements, and security flaw identification, tracking, and remediation processes.

Guidance

This control also applies to the development actions associated with information system changes.

Applicability: All	References: ARS: SA-10; NIST 800-53/53A: SA-10; PISP: 4.15.10	Related Controls:

ASSESSMENT PROCEDURE: SA-10.1

Assessment Objective

Determine if the organization requires that information system developers (and systems integrators) create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records.(Optional)

SA-11 – Developer Security Testing (Moderate)

Control

Information system developers shall develop, document, and implement a security test and evaluation (ST&E) plan for each information system under development in accordance with, but not limited to the, current CMS Procedures. The developer security test results shall be documented.

Guidance

Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant

modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system.

Applicability: All	**References:** FISCAM: TCC-2.1.5; NIST 800-53/53A: SA-11	**Related Controls:** CA-2, CA-4

ASSESSMENT PROCEDURE: SA-11.1

Assessment Objective

Determine if the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; other relevant documents or records.

SA-11(CMS-1) – Enhancement (Moderate)

Control

If the Security Test and Evaluation (ST&E) results are used in support of the security C&A process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the security testing and after selective verification of the results.

Applicability: All	**References:** ARS: SA-11(CMS-1); FISCAM: TCC-2.1.8	**Related Controls:**

ASSESSMENT PROCEDURE: SA-11(CMS-1).1

Assessment Objective

Determine if the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; other relevant documents or records to determine that no security relevant modifications of the information system has been made subsequent to the security testing and after selective verification of the results if the security test and evaluation results are used in support of the security C&A process for the information system.

Interview: Organizational personnel with developer security testing responsibilities to determine that no security relevant modifications of the information system has been made subsequent to the security testing and after selective verification of the results if the security test and evaluation results are used in support of the security C&A process for the information system.

SA-11(CMS-2) – Enhancement (Moderate)

Control

Use hypothetical data when executing test scripts.

Applicability: All	**References:** ARS: SI-7(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-11(CMS-2).1

Assessment Objective

Determine if the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records to determine hypothetical data is used when executing test scripts.

Interview: Personnel with system and information integrity responsibilities to determine hypothetical data is used when executing test scripts.

Test: Information systems to determine hypothetical data is used when executing test scripts.

System and Communications Protection (SC) – *Technical*

SC-1 – System and Communications Protection Policy and Procedures (Moderate)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: SC-1; FISCAM: TAC-3.2.E.1; IRS-1075: 5.6.3.4#1, 5.6.3.4#2; NIST 800-53/53A: SC-1; PISP: 4.16.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and communications protection policy and procedures;
(ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and
(iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and communications protection responsibilities.(Optional)

ASSESSMENT PROCEDURE: SC-1.2

Assessment Objective

Determine if:
(i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and communications protection responsibilities.(Optional)

SC-2 – Application Partitioning (Moderate)

Control

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Guidance

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Applicability: All	**References:** ARS: SC-2; NIST 800-53/53A: SC-2; PISP: 4.16.2	**Related Controls:**

ASSESSMENT PROCEDURE: SC-2.1

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Separation of user functionality from information system management functionality.(Optional)

SC-2(CMS-1) – Enhancement (Moderate)

Control

Place all CMS servers allowing public access within a DMZ environment, and disallow direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Applicability: All	**References:** ARS: SC-2(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-2(CMS-1).1

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Interview: Selected organizational personnel with network administration responsibilities to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Test: All CMS servers allowing public access to determine if the organization places these servers within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

SC-3 – Security Function Isolation (Moderate)

Control

Information system security functions shall be isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system shall maintain a separate execution domain (e.g., address space) for each executing process.

Guidance

The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Applicability: All	**References:** ARS: SC-3; NIST 800-53/53A: SC-3; PISP: 4.16.3	**Related Controls:**

ASSESSMENT PROCEDURE: SC-3.1

Assessment Objective

Determine if:

(i) the organization defines the security functions of the information system to be isolated from nonsecurity functions; and

(ii) the information system isolates security functions from nonsecurity functions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Separation of security functions from nonsecurity functions within the information system.(Optional)

SC-4 – Information Remnance (Moderate)

Control

No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.

Guidance

Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

Applicability: All	**References:** ARS: SC-4; IRS-1075: 5.6.3.4#2, 5.6.3.4#3; NIST 800-53/53A: SC-4; PISP: 4.16.4	**Related Controls:**

ASSESSMENT PROCEDURE: SC-4.1

Assessment Objective

Determine if the information system prevents unauthorized and unintended information transfer via shared system resources.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for unauthorized and unintended transfer of information via shared system resources.(Optional)

SC-4(0) – Enhancement (Moderate)

Control

Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Ensure that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure.

Applicability: All	**References:** ARS: SC-4(0); IRS-1075: 5.6.3.4#2; NIST 800-53/53A: SC-4; PISP: 4.16.4	**Related Controls:**

ASSESSMENT PROCEDURE: SC-4(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for unauthorized and unintended transfer of information via shared system resources.(Optional)

SC-4(PII-1) – Enhancement (Moderate)

Control

For PII, when authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting PII from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

Applicability: All	**References:** IRS-1075: 3.3#2	**Related Controls:**

ASSESSMENT PROCEDURE: SC-4(PII-1).1

Assessment Objective

Determine if the organization determines authorizations for further disclosures (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting PII from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

Assessment Methods And Objects

Examine: Bulk record identities which have been transmitted externally to another organization to determine if the records contain:

- approximate number of personal records
- date of the transmission
- best possible description of the records
- the name of the individuals making/receiving the transmission.

SC-5 – Denial of Service Protection (Moderate)

Control

Mechanisms shall be established to prevent, or limit the effects of well-known, detectable, and preventable denial-of-service attacks.

Guidance

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Applicability: All	**References:** ARS: SC-5; NIST 800-53/53A: SC-5; PISP: 4.16.5	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5.1

Assessment Objective

Determine if:
(i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and
(ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system for protection against or limitation of the effects of denial of service attacks.(Optional)

SC-5(0) – Enhancement (Moderate)

Control

Protect the information system against the denial-of-service attacks defined on the following sites or within the following documents:
- SANS Organization www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and
- NIST CVE List http://checklists.nist.gov/home.cfm.

Applicability: All	**References:** ARS: SC-5(0); NIST 800-53/53A: SC-5; PISP: 4.16.5	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan (for list of organization-defined types of denial of service attacks to protect against or limit); information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system for protection against or limitation of the effects of denial of service attacks.(Optional)

SC-5(1) – Enhancement (Moderate)

Control

Restrict the ability of users to launch denial of service attacks against other information systems or networks.

Applicability: All	**References:** ARS: SC-5(1); NIST 800-53/53A: SC-5(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5(1).1

Assessment Objective

Determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].(Optional)
Test: Information system for protection against or limitation of the effects of denial of service attacks].(Optional)

SC-5(2) – Enhancement (Moderate)

Control

Maintain excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

Applicability: All	**References:** ARS: SC-5(2); NIST 800-53/53A: SC-5(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5(2).1

Assessment Objective

Determine if the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].(Optional)

SC-6 – Resource Priority (Moderate)

Control

Mechanisms shall be implemented to provide for allocation of information system resources based upon priority. Priority protection shall ensure that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.

Applicability: All	**References:** ARS: SC-6; FISCAM: TSC-1.1; NIST 800-53/53A: SC-6; PISP: 4.16.6	**Related Controls:**

ASSESSMENT PROCEDURE: SC-6.1

Assessment Objective

Determine if the information system limits the use of resources by priority.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing prioritization of information system resources; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SC-7 – Boundary Protection (Moderate)

Control

Automated boundary protection mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces. The operational failure of the boundary protection mechanisms shall not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing site shall provide the same levels of protection as those of the primary site.

Guidance

Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.
The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-77 provides guidance on virtual private networks.

Applicability: All	**References:** ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	**Related Controls:** AC-4, CA-3, MP-4, RA-2

ASSESSMENT PROCEDURE: SC-7.1

Assessment Objective

Determine if:
(i) the organization defines key internal boundaries of the information system; and
(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Selected organizational personnel with boundary protection responsibilities.
Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system.(Optional)

SC-7(1) – Enhancement (Moderate)

Control

Physically allocate publicly-accessible information system components (e.g., public web servers, public email servers, public DNS servers) to separate sub-networks with separate physical network

interfaces.

Guidance

Publicly accessible information system components include, for example, public web servers.

Applicability: All	**References:** ARS: SC-7(1); NIST 800-53/53A: SC-7(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(1).1

Assessment Objective

Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records.

SC-7(2) – Enhancement (Moderate)

Control

Prevent public access into the internal networks except as appropriately mediated.

Applicability: All	**References:** ARS: SC-7(2); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(2).1

Assessment Objective

Determine if:
(i) the organization defines the mediation necessary for public access to the organization's internal networks; and
(ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing access controls for public access to the organization's internal networks.(Optional)

SC-7(3) – Enhancement (Moderate)

Control

Limit the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

Applicability: All	**References:** ARS: SC-7(3); NIST 800-53/53A: SC-7(3)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(3).1

Assessment Objective

Determine if the organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-7(4) – Enhancement (Moderate)

Control

Maintain a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

Applicability: All	**References:** ARS: SC-7(4); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(4)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(4).1

Assessment Objective

Determine if:
(i) the organization defines the security controls (i.e., boundary protection devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service; and
(ii) the organization implements a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.(Optional)

SC-7(5) – Enhancement (Moderate)

Control

Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.

Applicability: All	**References:** ARS: SC-7(5); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(5)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(5).1

Assessment Objective

Determine if the information system denies network traffic by default and allows network traffic by exception.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.(Optional)

SC-7(CMS-1) – Enhancement (Moderate)

Control

Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Applicability: All	**References:** ARS: SC-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(CMS-1).1

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; and automated mechanisms implementing boundary protection capability within the information system to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

SC-7(CMS-2) – Enhancement (Moderate)

Control

Utilize stateful inspection / application firewall hardware and software.

Applicability: All	**References:** ARS: SC-7(CMS-2); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(CMS-2).1

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; and automated mechanisms implementing boundary protection capability within the information system to determine if the organization utilizes stateful inspection / application firewall hardware and software.

SC-7(CMS-3) – Enhancement (Moderate)

Control

Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Applicability: All	**References:** ARS: SC-7(CMS-3)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(CMS-3).1

Assessment Objective

Determine if the organization defines key internal boundaries of the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

SC-8 – Transmission Integrity (Moderate)

Control

Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the integrity of CMS information while in transit.

Guidance

If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission integrity using IPSec. NIST SP 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Applicability: All	**References:** ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PISP: 4.16.8	**Related Controls:**

ASSESSMENT PROCEDURE: SC-8.1

Assessment Objective

Determine if the information system protects the integrity of transmitted information.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Transmission integrity capability within the information system.(Optional)

SC-8(1) – Enhancement (Moderate)

Control

Employ approved cryptographic mechanisms to ensure recognition of changes to information during transmission.

Applicability: All	**References:** ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(c)(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-8(1).1

Assessment Objective

Determine if the information system employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Cryptographic mechanisms implementing transmission integrity capability within the information system.(Optional)

SC-8(CMS-1) – Enhancement (Moderate)		
Control Employ appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13).		
Applicability: All	**References:** ARS: SC-8(CMS-1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(c)(1), 164.312(e)(2)(i)	**Related Controls:** SC-13
ASSESSMENT PROCEDURE: SC-8(CMS-1).1		
Assessment Objective Determine if the information system protects the integrity of transmitted information. **Assessment Methods And Objects** **Examine:** System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization employs appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13). **Interview:** Network administrators to determine if the organization employs appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13). **Test:** Transmission integrity capability within the information system to determine if the organization employs appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13).		
SC-9 – Transmission Confidentiality (Moderate)		
Control Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the confidentiality of CMS sensitive information while in transit.		
Guidance If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission confidentiality using IPSec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.		
Applicability: All	**References:** ARS: SC-9; HIPAA: 164.312(e)(1); IRS-1075: 5.6.3.4#2, 5.6.3.4#4.1; NIST 800-53/53A: SC-9; PISP: 4.16.9	**Related Controls:** AC-17
ASSESSMENT PROCEDURE: SC-9.1		
Assessment Objective Determine if the information system protects the confidentiality of transmitted information. **Assessment Methods And Objects** **Examine:** System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records. **Test:** Transmission confidentiality capability within the information system.(Optional)		
SC-9(1) – Enhancement (Moderate)		
Control Encryption is not required within a secured network. When transmitting data outside of a secured network: (a) An approved encryption method must be used (see SC-13, Use of Cryptography, PISP 4.16.13) (see SC-CMS-4 for E-Mail), and (b) Either a VPN or dedicated leased lines/circuits must be used.		
Applicability: All	**References:** ARS: SC-9(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(e)(1), 164.312(e)(2)(ii); IRS-1075: 5.6.3.4#2, 5.7#1	**Related Controls:** SC-13
ASSESSMENT PROCEDURE: SC-9(1).1		
Assessment Objective Determine if the information system employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measure.		

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Cryptographic mechanisms implementing transmission confidentiality capability within the information system.(Optional)

SC-9(PII-1) – Enhancement (Moderate)

Control

When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Applicability: All	**References:** IRS-1075: 5.7.4#1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-9(PII-1).1

Assessment Objective

Determine if the organization sending and receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Assessment Methods And Objects

Examine: Fax machine locations for secure custodial coverage of outgoing and incoming PII transmitted data.

Test: Send or receive a simulated PII fax to ensure that:
(i) a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines is located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients is maintained; and (iii) a cover sheet is used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

SC-10 – Network Disconnect (Moderate)

Control

Technical controls shall be established and implemented effectively to ensure that network connections are properly terminated at the end of user sessions, or upon the occurrence of specified conditions (e.g., a period of inactivity).

Guidance

The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Applicability: All	**References:** ARS: SC-10; NIST 800-53/53A: SC-10; PISP: 4.16.10	**Related Controls:**

ASSESSMENT PROCEDURE: SC-10.1

Assessment Objective

Determine if:
(i) the organization defines the time period of inactivity before the information system terminates a network connection; and
(ii) the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.

Test: Network disconnect capability within the information system.

SC-10(0) – Enhancement (Moderate)

Control

Configure the information system to forcibly disconnect network connections at the end of a session, or after fifteen (15) minutes of inactivity, for mainframe sessions.

Applicability: All	**References:** ARS: SC-10(0); FISCAM: TAC-3.2.C.3; NIST 800-53/53A: SC-10; PISP: 4.16.10	**Related Controls:**

ASSESSMENT PROCEDURE: SC-10(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.

Test: Network disconnect capability within the information system.

SC-11 – Trusted Path (Moderate)

Control

Technical controls shall be established and implemented effectively to provide the capability to establish trusted communications paths between authorized users and the security functionality of the information system.

Guidance

A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Applicability: All	**References:** ARS: SC-11; NIST 800-53/53A: SC-11; PISP: 4.16.11	**Related Controls:**

ASSESSMENT PROCEDURE: SC-11.1

Assessment Objective

Determine if:

(i) the organization defines the security functions within the information system that are included in a trusted communications path;

(ii) the organization-defined security functions include information system authentication and reauthentication; and

(iii) the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing trusted communications paths; information system security plan; information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing trusted communications paths within the information system.(Optional)

SC-11(0) – Enhancement (Moderate)

Control

At a minimum, a trusted communications path is established between the user and the following system security functions: system authentication, re-authentication, and key management.

Applicability: All	**References:** ARS: SC-11(0); FISCAM: TAC-3.2.E.1; PISP: 4.16.11	**Related Controls:**

ASSESSMENT PROCEDURE: SC-11(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing trusted communications paths; information system security plan (for organization-defined security functions to include for authentication and reauthentication); information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records.

Test: Automated mechanisms implementing trusted communications paths within the information system.

SC-12 – Cryptographic Key Establishment and Management (Moderate)

Control

When cryptography is required and used within the information system, documented procedures shall be implemented effectively for cryptographic key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect sensitive information shall be controlled and distributed using the NIST SP 800-56 and NIST SP 800-57 approved key management guidance.

Guidance

NIST SP 800-56 provides guidance on cryptographic key establishment. NIST SP 800-57 provides guidance on cryptographic key management.

Applicability: All	**References:** ARS: SC-12; IRS-1075: 5.7.1#1; NIST 800-53/53A: SC-12; PISP: 4.16.12	**Related Controls:**

ASSESSMENT PROCEDURE: SC-12.1

Assessment Objective

Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST SP 800-56 and 800-57; information system design

documentation; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel with responsibilities for cryptographic key establishment or management.(Optional)
Test: Automated mechanisms implementing cryptographic key management and establishment within the information system.(Optional)

SC-12(CMS-1) – Enhancement (Moderate)

Control

Employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall prohibit the use of encryption keys that are not recoverable by authorized personnel, require senior management approval to authorize recovery of keys by other than the key owner, and comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Applicability: All	References: ARS: SC-12(CMS-1)	Related Controls: MA-CMS-1, MA-CMS-2, SC-13

ASSESSMENT PROCEDURE: SC-12(CMS-1).1

Assessment Objective

Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).
Interview: A sample of organizational personnel with responsibilities for cryptographic key establishment or management to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).
Test: Automated mechanisms implementing cryptographic key management and establishment within the information system to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

SC-13 – Use of Cryptography (Moderate)

Control

When cryptographic mechanisms are used, procedures shall be developed, documented, and implemented effectively to ensure they comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. All such mechanisms shall be FIPS 140-2 (as amended and revised) compliant and NIST validated.

Guidance

The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	References: ARS: SC-13; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2, 5.6.3.4#4.2-3; NIST 800-53/53A: SC-13; PISP: 4.16.13	Related Controls: AC-17(CMS-1), AC-19(CMS-1), AC-3, AC-3(CMS-1), MP-4(PII-1), SC-12(CMS-1), SC-8(CMS-1), SC-9(1)

ASSESSMENT PROCEDURE: SC-13.1

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

SC-14 – Public Access Protections (Moderate)

Control

Technical controls shall be developed, documented, and implemented effectively to protect the integrity of the publicly accessible CMS information and applications.

Guidance

CMS refers to the National Institute of Standards and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix A provides a summary for remote access controls.

Applicability: All	**References:** ARS: SC-14; NIST 800-53/53A: SC-14; PISP: 4.16.14	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14.1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing access controls and boundary protection for publicly available information and applications within the information system.(Optional)

SC-14(CMS-1) – Enhancement (Moderate)

Control

Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

Applicability: All	**References:** ARS: SC-14(CMS-1); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14(CMS-1).1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

Interview: Organizational personnel to determine if network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

Test: Interfaces for all public-facing networks to determine if network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

SC-14(CMS-2) – Enhancement (Moderate)

Control

If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.

Applicability: All	**References:** ARS: SC-14(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14(CMS-2).1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.

Interview: MA owners for each public-facing MA to determine if e-authentication is required and implemented in conjunction with or related to public access protections; refer to ARS Appendix A for e-Authentication Standards.

Test: All public-facing systems to determine if e-authentication is required and implemented in conjunction with or related to public access protections; refer to ARS Appendix A for e-Authentication Standards.

SC-15 – Collaborative Computing (Moderate)

Control

Running collaborative computing mechanisms on CMS information systems shall require authorization by the CIO or his/her designated representative. The authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used. Collaborative computing mechanisms shall not be activated remotely.

Guidance

Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

Applicability: All	**References:** ARS: SC-15; NIST 800-53/53A: SC-15; PISP: 4.16.15	**Related Controls:**

ASSESSMENT PROCEDURE: SC-15.1

Assessment Objective

Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users.(Optional)

SC-15(1) – Enhancement (Moderate)

Control

If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:
Provide physical disconnect of cameras or microphones in a manner that supports ease of use.

Applicability: All	**References:** ARS: SC-15(1); NIST 800-53/53A: SC-15(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-15(1).1

Assessment Objective

Determine if the information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Physical disconnect of collaborative computing devices.(Optional)

SC-15(CMS-1) – Enhancement (Moderate)

Control

If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:
Ensure the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

Applicability: All	**References:** ARS: SC-15(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-15(CMS-1).1

Assessment Objective

Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

Interview: Personnel to determine if the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

Test: Automated mechanisms implementing access controls for collaborative computing environments and alert notification for local users to determine if the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

SC-16 – Transmission of Security Parameters (Moderate)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure that CMS information systems reliably associate security parameters with information exchanged between

information systems.

Guidance

Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Applicability: All	**References:** ARS: SC-16; NIST 800-53/53A: SC-16; PISP: 4.16.16	**Related Controls:**

ASSESSMENT PROCEDURE: SC-16.1

Assessment Objective

Determine if the information system reliably associates security parameters with information exchanged between information systems.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission of security parameters; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Automated mechanisms supporting reliable transmission of security parameters between information systems.(Optional)

SC-17 – Public Key Infrastructure Certificates (Moderate)

Control

All public key certificates used within the CMS information system shall be issued in accordance with a defined certification policy and certification practice statement. Registration to receive a public key certificate shall include authorization by a supervisor or a responsible official, and shall be done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

Guidance

For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24. NIST SP 800-32 provides guidance on public key technology. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**References:** ARS: SC-17; NIST 800-53/53A: SC-17; PISP: 4.16.17	**Related Controls:**

ASSESSMENT PROCEDURE: SC-17.1

Assessment Objective

Determine if the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; NIST SP 800-32; other relevant documents or records.

Interview: Organizational personnel with public key infrastructure certificate issuing responsibilities.(Optional)

SC-18 – Mobile Code (Moderate)

Control

CMS shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause harm to CMS information systems. The organization shall document, monitor, and implement controls for the use of mobile code within the CMS information system. Appropriate officials shall authorize or deny the use of mobile code. The organization shall implement controls and procedures for mobile code in accordance with NIST SP 800-28.

Guidance

Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST SP 800-28 provides guidance on active content and mobile code.

Applicability: All	**References:** ARS: SC-18; NIST 800-53/53A: SC-18; PISP: 4.16.18	**Related Controls:**

ASSESSMENT PROCEDURE: SC-18.1

Assessment Objective

Determine if:

(i) the organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and

(ii) the organization authorizes, monitors, and controls the use of mobile code within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation guidance; NIST SP 800-28; other relevant

documents or records.
Interview: Organizational personnel with mobile code authorization, monitoring, and control responsibilities.(Optional)
Test: Mobile code authorization and monitoring capability for the organization.(Optional)

SC-19 – Voice Over Internet Protocol (Moderate)

Control

CMS shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to harm CMS information systems. The organization shall document, monitor, and implement controls for the use of VoIP within a CMS information system. When VoIP is implemented, the organization shall adhere to the NIST SP 800-58 guidance.

Guidance

NIST SP 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.

Applicability: All	**References:** ARS: SC-19; NIST 800-53/53A: SC-19; PISP: 4.16.19	**Related Controls:**

ASSESSMENT PROCEDURE: SC-19.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and
(ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other relevant documents or records.
Interview: Organizational personnel with VoIP authorization and monitoring responsibilities.(Optional)

SC-19(CMS-1) – Enhancement (Moderate)

Control

The use of VoIP must be authorized in writing by the CMS CIO, or his/her designated representative.

Applicability: All	**References:** ARS: SC-19(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-19(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and
(ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; and other relevant documents or records to determine if the use of VoIP is authorized in writing by the CMS CIO, or his/her designated representative.
Interview: Organizational personnel with VoIP authorization and monitoring responsibilities to determine if the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

SC-20 – Secure Name / Address Resolution Service (Authoritative Source) (Moderate)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

Guidance

This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment.

Applicability: All	**References:** ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20	**Related Controls:**

ASSESSMENT PROCEDURE: SC-20.1

Assessment Objective

Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional

data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); NIST SP 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing secure name/address resolution service (authoritative source) within the information system.(Optional)

SC-22 – Architecture and Provisioning for Name / Address Resolution Service (Moderate)

Control

Information systems that collectively provide name / address resolution service for an organization shall be fault tolerant and implement role separation.

Guidance

A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified. NIST SP 800-81 provides guidance on secure DNS deployment.

Applicability: All	**References:** ARS: SC-22; NIST 800-53/53A: SC-22; PISP: 4.16.22	**Related Controls:**

ASSESSMENT PROCEDURE: SC-22.1

Assessment Objective

Determine if the information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; NIST SP 800-81; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms supporting name/address resolution service for fault tolerance and role separation.(Optional)

SC-23 – Session Authenticity (Moderate)

Control

Technical controls shall be developed, documented, and effectively implemented to ensure that CMS information systems provide mechanisms to protect the authenticity of communications sessions.

Guidance

This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST SP 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST SP 800-77 provides guidance on the deployment of IPSec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST SP 800-95 provides guidance on secure web services.

Applicability: All	**References:** ARS: SC-23; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-23; PISP: 4.16.23	**Related Controls:**

ASSESSMENT PROCEDURE: SC-23.1

Assessment Objective

Determine if the information system provides mechanisms to protect the authenticity of communications sessions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing session authenticity; NIST SP 800-52, 800-77, and 800-95; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing session authenticity.(Optional)

SC-CMS-1 – Desktop Modems (Moderate)

Control

Users are prohibited from installing desktop modems.

Guidance

Desktop Modems allow backdoors into the network putting the CMS data and network at very high risk.

Applicability: All	**References:** ARS: SC-CMS-1; PISP: 4.16.24	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-1.1

Assessment Objective

Determine if the organization has implement a policy which assists in prohibiting the installation of unauthorized desktop modems.

Assessment Methods And Objects

Examine: Organizational policy does not allow unauthorized desktop modems.

SC-CMS-2 – Identify and Detect Unauthorized Modems (Moderate)

Control

Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized modems.

Guidance

It is good practice that management approve any automated tool or utility for checking for unauthorized modems.

Applicability: All	**References:** ARS: SC-CMS-2; PISP: 4.16.25	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-2.1

Assessment Objective

Determine if the organization has an approved automated system to test for unauthorized modems.

Assessment Methods And Objects

Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

SC-CMS-2(CMS-0) – Enhancement (Moderate)

Control

Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly.

Applicability: All	**References:** ARS: SC-CMS-2(CMS-0)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less than quarterly.

SC-CMS-3 – Secondary Authentication and Encryption (Moderate)

Control

Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network.

Guidance

A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP.

Applicability: All	**References:** ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-3.1

Assessment Objective

Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit.

Assessment Methods And Objects

Examine: In-transit technical controls implement and documents for sensitive information outside the secure network.

SC-CMS-3(CMS-0) – Enhancement (Moderate)		
Control Enable application security mechanisms, such as Transport Layer Security (TLS). Utilize CMS-approved encryption and password authentication methods.		
Applicability: All	**References:** ARS: SC-CMS-3(CMS-0)	**Related Controls:**
ASSESSMENT PROCEDURE: SC-CMS-3(CMS-0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Documentation to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization utilizes CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric). **Interview:** Organizational personnel to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization utilizes CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric). **Test:** Information system to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization utilizes CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).		
SC-CMS-3(CMS-1) – Enhancement (Moderate)		
Control If e-authentication is required and implemented, refer to ARS Appendix A for e-Authentication Standards controls and procedures.		
Applicability: All	**References:** ARS: SC-CMS-3(CMS-1)	**Related Controls:**
ASSESSMENT PROCEDURE: SC-CMS-3(CMS-1).1		
Assessment Objective Determine if the organization that uses e-authentication is required to refer to ARS Appendix A for e-Authentication Standards controls and procedures. **Assessment Methods And Objects** **Examine:** Network documentation to determine which recommends enabling application security mechanisms, such as TLS, and utilizing minimum encryption and password authentication although, no specific requirements are mandatory. **Interview:** Organizational personnel to determine if enabling application security mechanisms is recommended, such as TLS, and utilizing minimum encryption and password authentication although, no specific requirements are mandatory. **Test:** Information system to determine if application security mechanisms are enabled, such as TLS, and the organization utilizes minimum encryption and password authentication although, no specific requirements are mandatory.		
SC-CMS-4 – Electronic Mail (Moderate)		
Control Controls shall be developed, documented, and implemented effectively to protect CMS sensitive information that is sent via e-mail.		
Guidance A good place to obtain technical controls for handling sensitive information via e-mail is the NIST SP.		
Applicability: All	**References:** ARS: SC-CMS-4; PISP: 4.16.27	**Related Controls:**
ASSESSMENT PROCEDURE: SC-CMS-4.1		
Assessment Objective Determine if the organization effectively develops, documents, and implements protections for CMS sensitive information that is sent via e-mail. **Assessment Methods And Objects** **Examine:** Documentation to determine if all e-mail messages with CMS sensitive information are transmitted using protective measures. **Interview:** Organizational personnel to determine if all e-mail messages with CMS sensitive information is protected, controlled, and monitored.		
SC-CMS-4(CMS-0) – Enhancement (Moderate)		
Control Prior to sending an email, place all CMS sensitive information in an encrypted attachment.		
Applicability: All	**References:** ARS: SC-CMS-4(CMS-0); IRS-1075: 5.7.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-4(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Documentation to determine if all e-mail messages are encrypted and verify encryption / decryption for received messages.

Interview: Organizational personnel to determine if all e-mail messages are encrypted, and encryption /decryption for received messages.

SC-CMS-5 – Persistent Cookies (Moderate)

Control

The use of persistent cookies on a CMS web site is prohibited unless explicitly approved in writing by the DHHS Secretary.

Guidance

Requests to DHHS should be via CMS.

Applicability: All	**References:** ARS: SC-CMS-5; PISP: 4.16.28	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-5.1

Assessment Objective

Determine if the organization does not use a persistent cookie configuration on a CMS web site to remember subsequent visits unless approved in writing by the DHHS Secretary.

Assessment Methods And Objects

Examine: CMS web site baseline and change management documentation for configurations using persistent cookies.

Interview: Web site administrators to determine if the CMS web site has persistent cookies enable in the baseline configuration or have written approval to enable persistent cookies from the DHHS Secretary.

SC-CMS-6 – Network Interconnection (Moderate)

Control

Controls shall be developed, documented, and implemented effectively to ensure that only properly authorized network interconnections external to the system boundaries are established.

Guidance

A good place to obtain technical controls for securing interconnections external to the system boundaries is the NIST SP.

Applicability: All	**References:** ARS: SC-CMS-6; PISP: 4.16.29	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-6.1

Assessment Objective

Determine if the organization effectively documents and implements authorized network interconnections external to the system boundaries.

Assessment Methods And Objects

Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards for all external interconnections.

SC-CMS-6(CMS-0) – Enhancement (Moderate)

Control

Ensure remote location(s) (e.g., users and sites using a network interconnection external to the system boundaries) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

Applicability: All	**References:** ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

Interview: Personnel to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

System and Information Integrity (SI) – *Operational*

SI-1 – System and Information Integrity Policy and Procedures (Moderate)

Control

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems, software, and information. The procedures and automated mechanisms shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. It is good practice to have an automated system which is host based to automatically detect, block/filter and alert supervisors or managers that possible unauthorized changes to software and the information system have occurred.

Applicability: All	**References:** ARS: SI-1; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-1; PISP: 4.17.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and information integrity policy and procedures;
(ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and information integrity policy and procedures; and
(iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and information integrity responsibilities.(Optional)

ASSESSMENT PROCEDURE: SI-1.2

Assessment Objective

Determine if:
(i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and information integrity responsibilities.(Optional)

SI-2 – Flaw Remediation (Moderate)

Control

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. The flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

Guidance

The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. It is a good practice to test the changes in a laboratory environment on like systems prior to approving and implementing the updates and changes. NIST SP 800-40, provides guidance on security patch installation and patch management.

Applicability: All	**References:** ARS: SI-2; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2; PISP: 4.17.2	**Related Controls:** CA-2, CA-4, CA-7, CM-3, IR-4, SI-11

ASSESSMENT PROCEDURE: SI-2.1

Assessment Objective

Determine if:
(i) the organization identifies, reports, and corrects information system flaws;
(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;
(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;
(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and
(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(0) – Enhancement (Moderate)

Control

Correct identified information system flaws on production equipment within one (1) week.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and
(b) Manage the flaw remediation process centrally.

Applicability: All	**References:** ARS: SI-2(0); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2; PISP: 4.17.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(1) – Enhancement (Moderate)

Control

Updates are installed automatically.

Applicability: All	**References:** ARS: SI-2(1); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-2(1).1

Assessment Objective

Determine if the organization centrally manages the flaw remediation process and installs updates automatically.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records.(Optional)

Test: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates.(Optional)

SI-2(2) – Enhancement (Moderate)

Control

Employ automated mechanisms periodically and upon demand to determine the state of information system components with regard to flaw remediation.

Applicability: All	**References:** ARS: SI-2(2); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-2(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system flaw remediation update status.

SI-3 – Malicious Code Protection (Moderate)

Control

Automated malicious code protection mechanisms that include a capability of automatic updates shall be in place and supporting procedures shall be developed, documented, and implemented effectively to identify and isolate suspected malicious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical information system entry points, and at each workstation, server, or mobile computing device on the network to detect and eradicate malicious code transported by email, email attachments, removable media or other methods. Business owners shall use antiviral software products from multiple vendors, if possible, and update virus protection mechanisms whenever new releases are available.

Guidance

The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST SP 800-83 provides guidance on implementing malicious code protection.

Applicability: All	**References:** ARS: SI-3; FISCAM: TCC-1.3.2; IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3.1

Assessment Objective

Determine if:

(i) the information system implements malicious code protection;

(ii) the organization employs malicious code protection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;

(iii) the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities;

(iv) the organization updates malicious code protection mechanisms whenever new releases are available; and

(v) the malicious code protection mechanisms are appropriately updated to include the latest malicious code definitions, configured to perform periodic scans of the information system as well as real-time scans of files from external sources as the files are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(0) – Enhancement (Moderate)

Control

Implement malicious code protection at information system entry points, including firewalls, email servers, remote access servers, workstations, servers, and mobile computing devices by employing automated mechanisms to detect and eradicate malicious code transported by email, email attachments, and removable media.

Applicability: All	**References:** ARS: SI-3(0); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection

updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(1) – Enhancement (Moderate)

Control

Manage and update malicious code protection software centrally with automatic updates for the latest malicious code definitions whenever new releases are available.

Applicability: All	**References:** ARS: SI-3(1); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(1).1

Assessment Objective

Determine if the organization centrally manages malicious code protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(2) – Enhancement (Moderate)

Control

Employ automated mechanisms to update malicious code protection.

Applicability: All	**References:** ARS: SI-3(2); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3(2)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(2).1

Assessment Objective

Determine if the organization automatically updates malicious code protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automatic update capability for malicious code protection.

SI-3(CMS-1) – Enhancement (Moderate)

Control

Enable real-time file scanning. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and every twenty-four (24) hours.

Applicability: All	**References:** ARS: SI-3(CMS-1); IRS-1075: 5.6.2.5#1.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(CMS-1).1

Assessment Objective

Determine if:
(i) real-time file scanning is enabled;
(ii) real-time desktop malicious code scanning is enabled and monitored; and
(iii) software is configured to perform critical system file scans during system boot and every twenty-four (24) hours.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records to determine real-time file scanning is enabled. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and every twenty-four (24) hours.

Interview: Personnel with system and information integrity responsibilities to determine real-time file scanning is enabled, desktop malicious code scanning software is installed, real-time protection, and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and every twenty-four (24) hours.

Test: Information system real-time file scanning is enabled, desktop malicious code scanning software is installed, real-time protection, and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and every twenty-four (24) hours.

SI-4 – Information System Monitoring Tools and Techniques (Moderate)

Control

Effective monitoring tools and techniques providing real-time identification of unauthorized use, misuse, and abuse of the information system shall be implemented.

Guidance

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST SP 800-61 provides guidance on detecting attacks through various types of security technologies. NIST SP 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST SP 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST SP 800-94 provides guidance on intrusion detection and prevention.

Applicability: All	**References:** ARS: SI-4; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4; PISP: 4.17.4	**Related Controls:** AC-8, AU-4, CM-6

ASSESSMENT PROCEDURE: SI-4.1

Assessment Objective

Determine if the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

SI-4(1) – Enhancement (Moderate)

Control

Connect individual IDS devices to a common IDS management network using common protocols.

Applicability: All	**References:** ARS: SI-4(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(1).1

Assessment Objective

Determine if the organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.(Optional)

Test: Information system-wide intrusion detection capability.(Optional)

SI-4(4) – Enhancement (Moderate)

Control

Monitor inbound and outbound communications for unusual or unauthorized activities or conditions.

Guidance

Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.

Applicability: All	**References:** ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(4).1

Assessment Objective

Determine if:

(i) the organization identifies the types of activities or conditions considered unusual or unauthorized; and

(ii) the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; types of activities or conditions considered unusual or unauthorized; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system monitoring capability for inbound and outbound communications.

SI-4(5) – Enhancement (Moderate)

Control

Real-time alerts are provided when indications of the following types of compromise, or potential compromise, occur:
(a) Presence of malicious code,
(b) Unauthorized export of information,
(c) Signaling to an external information system, or
(d) Potential intrusions.

Applicability: All	**References:** ARS: SI-4(5)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(5).1

Assessment Objective

Determine if:
(i) the organization identifies indications of compromise or potential compromise to the security of the information system; and
(ii) the information system provides a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Information system monitoring real-time alert capability.(Optional)

SI-4(CMS-1) – Enhancement (Moderate)

Control

Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.

Applicability: All	**References:** ARS: SI-4(CMS-1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(CMS-1).1

Assessment Objective

Determine if:
(i) IDS devices are installed at network perimeter points; and
(ii) host-based IDS sensors are installed on critical servers.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.
Interview: Personnel with system and information integrity responsibilities to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.
Test: Information system-wide intrusion detection capability to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

SI-5 – Security Alerts and Advisories (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis, and for issuing IS alerts and advisories to appropriate personnel. Upon receipt of such alerts and advisories, personnel shall take appropriate response actions. The types of actions to be taken in response to security alerts / advisories shall be documented.

Guidance

The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST SP 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Applicability: All	**References:** ARS: SI-5; NIST 800-53/53A: SI-5; PISP: 4.17.5	**Related Controls:**

ASSESSMENT PROCEDURE: SI-5.1

Assessment Objective

Determine if:
(i) the organization receives information system security alerts/advisories on a regular basis;

(ii) the organization issues security alerts/advisories to appropriate organizational personnel; and
(iii) the organization takes appropriate actions in response to security alerts/advisories.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; NIST SP 800-40; records of security alerts and advisories; other relevant documents or records.

Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system.

SI-5(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to make security alerts and advisory information available to all appropriate personnel.

Applicability: All	**References:** ARS: SI-5(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-5(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing the distribution of security alert and advisory information.(Optional)

SI-6 – Security Functionality Verification (Moderate)

Control

Automated mechanisms shall be established and implemented effectively to provide the capability for CMS information systems to verify the correct operation of security functions on a regular basis, and automatically to take appropriate response actions when security-related anomalies are discovered.

Guidance

The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Applicability: All	**References:** ARS: SI-6; NIST 800-53/53A: SI-6; PISP: 4.17.6	**Related Controls:**

ASSESSMENT PROCEDURE: SI-6.1

Assessment Objective

Determine if:
(i) the organization defines the appropriate conditions for conducting security function verification;
(ii) the organization defines, for periodic security function verification, the frequency of the verifications;
(iii) the organization defines information system responses to anomalies discovered during security function verification;
(iv) the information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification); and
(v) the information system responds to security function anomalies in accordance with organization-defined responses.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Security function verification capability.(Optional)

SI-7 – Software and Information Integrity (Moderate)

Control

Automated mechanisms for software and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to software. Good software engineering practices consistent with CMS IS policy and procedures shall be employed with regard to commercial-off-the-shelf (COTS) integrity mechanisms, and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications.

Guidance

The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the

integrity of the information system and the applications it hosts.

Applicability: All	**References:** ARS: SI-7; FISCAM: TAN-3.1.2, TAN-3.2.1, TAN-3.2.2, TAY-2.1.4, TAY-2.2.2, TCP-2.1.2, TCP-2.1.3, TCP-2.1.4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7; PISP: 4.17.7	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7.1

Assessment Objective

Determine if:
(i) the information system detects and protects against unauthorized changes to software and information; and
(ii) the organization employs effective integrity verification tools in accordance with good software engineering practices.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records.(Optional)
Test: Software integrity protection and verification capability.(Optional)

SI-7(0) – Enhancement (Moderate)

Control

Employ off-the-shelf integrity mechanisms such as parity checks, check-sums, error detection data validation techniques, cyclical redundancy checks, and cryptographic hashes to detect and protect against information tampering, errors, omissions and unauthorized changes to software and use tools to automatically monitor the integrity of the information system and the application it hosts.

Applicability: All	**References:** ARS: SI-7(0); FISCAM: TAC-3.3; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); PISP: 4.17.7	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records.

SI-7(FIS-1) – Enhancement (Moderate)

Control

A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing. Live data are not used in testing of program changes except to build test data files.

Applicability: All	**References:** FISCAM: TCC-2.1.6, TCC-2.1.7	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-1).1

Assessment Objective

Determine if:
(i) the organization provides a comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.
(ii) the organizational validation does not use live data in testing of program changes except to build test data files.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Test transactions and data.
Interview: Programmers, auditors, and quality assurance personnel.

SI-7(FIS-2) – Enhancement (Moderate)

Control

User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.

Applicability: All	**References:** FISCAM: TCP-1.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-2).1

Assessment Objective

Determine if the organizational user-prepared record count and control totals documents help determine the completeness of data entry and processing.

Assessment Methods And Objects

Examine: Activity for developing record counts and control totals.

Examine: Application documentation.
Examine: Pertinent policies and procedures.
Interview: User management and personnel.

SI-7(FIS-3) – Enhancement (Moderate)

Control

For on-line or real-time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing.

Applicability: All	**References:** FISCAM: TCP-1.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-3).1

Assessment Objective

Determine if the organizational on-line or real-time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing.

Assessment Methods And Objects

Examine: Application documentation.
Examine: Pertinent policies and procedures.
Examine: Supporting documentation generated by system.
Interview: Application programmer, if available.
Interview: User management and personnel.

SI-7(FIS-4) – Enhancement (Moderate)

Control

Record counts and control totals are established over and entered with transaction data, and reconciled to determine the completeness of data entry.

Applicability: All	**References:** FISCAM: TCP-2.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-4).1

Assessment Objective

Determine if the organizational record counts and control totals are established over and entered with transaction data, and reconciled to determine the completeness of data entry.

Assessment Methods And Objects

Examine: Application documentation.
Examine: Pertinent policies and procedures.
Examine: Reconciliation activities.
Interview: Data control personnel.
Interview: User management and personnel.

SI-7(FIS-5) – Enhancement (Moderate)

Control

Reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated.

Applicability: All	**References:** FISCAM: TCP-2.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-5).1

Assessment Objective

Determine if the organizational reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated.

Assessment Methods And Objects

Examine: Application documentation.
Examine: Pertinent policies and procedures.
Examine: Reconciliation activities.
Interview: Data control personnel.
Interview: User management and personnel.

SI-8 – Spam Protection (Moderate)

Control

Automated mechanisms for spam protection shall be in place at critical information system entry points, workstations, servers, and mobile computing devices on the network. Supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect spam.

Guidance

The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST SP 800-45 provides guidance on electronic mail security.

Applicability: All	**References:** ARS: SI-8; HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8; PISP: 4.17.8	**Related Controls:**

ASSESSMENT PROCEDURE: SI-8.1

Assessment Objective

Determine if:
(i) the information system implements spam protection;
(ii) the organization employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network;
(iii) the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail; and
(iv) the organization updates spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

Test: Spam detection and handling capability.

SI-8(1) – Enhancement (Moderate)

Control

Centrally manage spam protection mechanisms.

Applicability: All	**References:** ARS: SI-8(1); HIPAA: 164.308(a)(1)(i)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-8(1).1

Assessment Objective

Determine if the organization centrally manages spam protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SI-9 – Information Input Restrictions (Moderate)

Control

Automated mechanisms shall be in place to restrict information input to the information system to authorized personnel. Personnel authorized to input information to the information system shall be restricted beyond the typical access controls employed by the system, including limitations based on specific operational / project responsibilities.

Guidance

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Applicability: All	**References:** ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.1; NIST 800-53/53A: SI-9; PISP: 4.17.9	**Related Controls:**

ASSESSMENT PROCEDURE: SI-9.1

Assessment Objective

Determine if the organization restricts the capability to input information to the information system to authorized personnel.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SI-10 – Information Accuracy, Completeness, Validity, and Authenticity (Moderate)

Control

Automated mechanisms shall verify information for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

Guidance

Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Applicability: All	**References:** ARS: SI-10; FISCAM: TAN-3.1.1, TAY-1.2.1, TAY-1.4.1, TAY-2.1.3, TCP-2.1.2, TCP-2.1.3, TCP-2.1.4; IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-10; PISP: 4.17.10	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10.1

Assessment Objective

Determine if:
(i) the information system checks information for accuracy, completeness, validity, and authenticity;
(ii) checks for accuracy, completeness, validity, and authenticity of information is accomplished as close to the point of origin as possible;
(iii) the information system employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions for format and content; and
(iv) the information system prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system capability for checking information for accuracy, completeness, validity, and authenticity.(Optional)

SI-10(CMS-1) – Enhancement (Moderate)

Control

Implement automated system checks of information for accuracy, completeness, validity, and authenticity.

Applicability: All	**References:** ARS: SI-10(CMS-1); FISCAM: TAN-3.1.1, TCP-2.1.3, TCP-2.1.4; IRS-1075: 5.6.2.5#1.1-2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(CMS-1).1

Assessment Objective

Determine if the information system checks information for accuracy, completeness, validity, and authenticity.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine that automated system checks of information for accuracy, completeness, validity, and authenticity are performed.
Interview: Personnel with system and information integrity responsibilities to determine that automated system checks of information for accuracy, completeness, validity, and authenticity are performed.
Test: Information system to determine that automated system checks of information for accuracy, completeness, validity, and authenticity are performed.

SI-10(FIS-1) – Enhancement (Moderate)

Control

The source document is well-designed to aid the preparer and facilitate data entry and includes document pre-numbering and preprinting of transaction type and data field codes. The document numbers, transaction types and field codes are entered into the system to facilitate completeness and sequence checking. Access to blank source documents is restricted to authorized personnel.

Applicability: All	**References:** FISCAM: TAN-1.1.1, TAN-1.1.2, TAN-1.1.3, TAY-1.1.1, TAY-1.1.2, TCP-1.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-1).1

Assessment Objective

Determine if the organizational source document is well-designed to aid the preparer and facilitate data entry and includes document pre-numbering and preprinting of transaction type and data field codes. The document numbers, transaction types and field codes are entered into the system to facilitate completeness and sequence checking. Access to blank source documents is restricted to

authorized personnel.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Blank document storage area.
Examine: Procedures for recording and tracking of numbers if pre-numbered documents are used.
Examine: Source documents and data entry activities.
Interview: User management and personnel.

SI-10(FIS-2) – Enhancement (Moderate)

Control

For batch application systems, a batch control sheet is prepared for a group of source documents, and includes: date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.

Applicability: All	**References:** FISCAM: TAN-1.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-2).1

Assessment Objective

Determine if the organizational batch application systems prepared a batch control sheet for a group of source documents, and includes: date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Batch control sheets if batch application.
Examine: Prepared source documents and batches if batch application.
Interview: Users responsible for preparing batch control sheets and submitting the batch.

SI-10(FIS-3) – Enhancement (Moderate)

Control

Key source documents require authorizing signatures. Data control unit personnel: verify that source documents are properly prepared and authorized; and monitor data entry and processing of source documents.

Applicability: All	**References:** FISCAM: TAN-1.2.1, TAN-1.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-3).1

Assessment Objective

Determine if the organizational key source documents require authorizing signatures. Data control unit personnel: verify that source documents are properly prepared and authorized; and monitor data entry and processing of source documents.

Assessment Methods And Objects

Examine: Key source documents and data entry activities.
Examine: Pertinent policies and procedures.
Interview: Management and data control unit personnel.

SI-10(FIS-4) – Enhancement (Moderate)

Control

Supervisory or control unit personnel review data and enter an authorizing code before data is released for processing.

Applicability: All	**References:** FISCAM: TAN-1.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-4).1

Assessment Objective

Determine if the organizational supervisory or control unit personnel review data and enter an authorizing code before data is released for processing.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Review process.
Interview: Management and data control unit personnel.

SI-10(FIS-5) – Enhancement (Moderate)		
Control Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.		
Applicability: All	**References:** FISCAM: TAY-2.3.2	**Related Controls:**
ASSESSMENT PROCEDURE: SI-10(FIS-5).1		
Assessment Objective Determine if the organization information system override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Override audit logs. **Interview:** Application programmer, if available, and user management personnel.		
SI-10(FIS-6) – Enhancement (Moderate)		
Control Transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.		
Applicability: All	**References:** FISCAM: TCP-1.2.2	**Related Controls:**
ASSESSMENT PROCEDURE: SI-10(FIS-6).1		
Assessment Objective Determine if the organizational information system transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Pertinent policies and procedures. **Examine:** Supporting documentation generated by system. **Interview:** Application programmer, if available. **Interview:** User management and personnel.		
SI-10(FIS-7) – Enhancement (Moderate)		
Control Transactions are sequence checked and computer matched with data in master or suspense files to identify missing or duplicate transactions. Reports of missing or duplicate transactions are produced, and items are investigated and resolved in a timely manor.		
Applicability: All	**References:** FISCAM: TCP-1.2.3, TCP-1.2.4, TCP-1.3.1, TCP-1.3.2	**Related Controls:**
ASSESSMENT PROCEDURE: SI-10(FIS-7).1		
Assessment Objective Determine if the organizational information system transactions are sequence checked and computer matched with data in master or suspense files to identify missing or duplicate transactions. Reports of missing or duplicate transactions are produced, and items are investigated and resolved in a timely manor. **Assessment Methods And Objects** **Examine:** Activity to investigate items reported as missing or duplicate. **Examine:** Application documentation. **Examine:** Pertinent policies and procedures. **Examine:** Reports of missing and duplicate transactions. **Interview:** Application programmer, if available. **Interview:** User management and personnel.		
SI-10(FIS-8) – Enhancement (Moderate)		
Control Individual transactions or source documents are compared with a detailed listing of items processed by the computer, particularly to control important low-volume, high-value transactions.		
Applicability: All	**References:** FISCAM: TCP-1.4.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-10(FIS-8).1

Assessment Objective

Determine if the organizational information system's individual transactions or source documents are compared with a detailed listing of items processed by the computer, particularly to control important low-volume, high-value transactions.

Assessment Methods And Objects

Examine: Comparison activity.
Examine: Listings for notations showing checking was performed.
Examine: Pertinent policies and procedures.
Interview: User management and personnel.

SI-11 – Error Handling (Moderate)

Control

Information systems shall identify and handle error conditions in an expeditious manner. User error messages generated by information systems shall provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages shall be revealed only to authorized personnel. Sensitive information shall not be listed in error logs or associated administrative messages.

Guidance

The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Applicability: All	**References:** ARS: SI-11; FISCAM: TAY-3.2.1; NIST 800-53/53A: SI-11; PISP: 4.17.11	**Related Controls:** SI-2

ASSESSMENT PROCEDURE: SI-11.1

Assessment Objective

Determine if:
(i) the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries;
(ii) the information system reveals only essential information to authorized individuals; and
(iii) the information system does not include sensitive information in error logs or associated administrative messages.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system error handling capability.(Optional)

SI-11(0) – Enhancement (Moderate)

Control

Employ automated mechanisms that generate error messages providing timely and useful information to users without revealing information that could be exploited by adversaries. Ensure confidential information (e.g., account numbers, User IDs, social security numbers, etc.) is not listed in error logs or associated with administrative messages.

Applicability: All	**References:** ARS: SI-11(0); FISCAM: TAY-4.1.8; NIST 800-53/53A: SI-11; PISP: 4.17.11	**Related Controls:**

ASSESSMENT PROCEDURE: SI-11(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SI-11(FIS-1) – Enhancement (Moderate)

Control

Rejected data are automatically written on an automated error suspense file and purged as corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error, (2) date and time the transaction was processed and the error identified, and (3) the identity of the user who originated the transaction. Record counts and control totals are established over the suspense file and used in reconciling transactions processed.

Applicability: All	**References:** FISCAM: TAY-3.1.1, TAY-3.1.2, TAY-3.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: SI-11(FIS-1).1

Assessment Objective

Determine if the organizational information system's rejected data is automatically written on an automated error suspense file and purged as corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error, (2) date and time the transaction was processed and the error identified, and (3) the identity of the user who originated the transaction. Record counts and control totals are established over the suspense file and used in reconciling transactions processed.

Assessment Methods And Objects

Examine: Application documentation and interview application programmers, if available.
Examine: Reports produced from the suspense file.
Interview: User management and personnel.
Test: Verify process with test transactions containing errors.

SI-11(FIS-2) – Enhancement (Moderate)

Control

A control group is responsible for: reviewing suspense file control total reports, determining completeness of processing, and controlling and monitoring rejected transactions

Applicability: All	**References:** FISCAM: TAY-3.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-11(FIS-2).1

Assessment Objective

Determine if the organizational information system's control group is responsible for: reviewing suspense file control total reports, determining completeness of processing, and controlling and monitoring rejected transactions

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Reports produced from the suspense file.
Interview: User management and control group.
Test: Verify review process with test transactions containing errors.

SI-11(FIS-3) – Enhancement (Moderate)

Control

The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected transactions.

Applicability: All	**References:** FISCAM: TAY-3.1.5	**Related Controls:**

ASSESSMENT PROCEDURE: SI-11(FIS-3).1

Assessment Objective

Determine if:
(i) the organizational information system [The suspense file] is produced, on a regular basis for management review; and
(ii) the organization determines the level and type of transaction errors and the age of uncorrected transactions.

Assessment Methods And Objects

Examine: Analysis reports produced from the suspense file.
Examine: Application documentation.
Examine: Pertinent policies and procedures.
Interview: User management and control group.

SI-11(FIS-4) – Enhancement (Moderate)

Control

Errors are corrected by the user originating the transaction, and all corrections are reviewed and approved by supervisors before the corrections are reentered.

Applicability: All	**References:** FISCAM: TAY-3.2.2, TAY-3.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-11(FIS-4).1

Assessment Objective

Determine if the organizational information system errors are corrected by the user originating the transaction, and all corrections are reviewed and approved by supervisors before the corrections are reentered.

Assessment Methods And Objects

Examine: Error correction activities.
Examine: Error reports.
Examine: Pertinent policies and procedures.
Interview: User management and personnel.
Test: Verify test transactions containing errors.

SI-11(FIS-5) – Enhancement (Moderate)

Control

A control group is responsible for: reviewing control total reports, determining completeness of processing, and controlling and monitoring rejected transactions

Applicability: All	**References:** FISCAM: TCP-2.1.5	**Related Controls:**

ASSESSMENT PROCEDURE: SI-11(FIS-5).1

Assessment Objective

Determine if the organizational control group is responsible for: reviewing control total reports, determining completeness of processing, and controlling and monitoring rejected transactions

Assessment Methods And Objects

Examine: Application documentation.
Examine: Pertinent policies and procedures.
Examine: Review and completeness of processing activities.
Interview: Data control personnel.
Interview: User management and personnel.

SI-12 – Information Output Handling and Retention (Moderate)

Control

Output from information systems shall be handled and retained in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, operational requirements, and the information sensitivity level.

Guidance

A good place to obtain procedures for handling sensitive output information is the NIST SP.

Applicability: All	**References:** ARS: SI-12; FISCAM: TAY-4.1.6; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2; NIST 800-53/53A: SI-12; PISP: 4.17.12	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12.1

Assessment Objective

Determine if:
(i) the organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and
(ii) the organization handles output from the information system in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records.
Interview: Organizational personnel with information output handling and retention responsibilities.(Optional)

SI-12(CMS-1) – Enhancement (Moderate)

Control

Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements.

Applicability: All	**References:** ARS: SI-12(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12(CMS-1).1

Assessment Objective

Determine if the organization retains output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable NARA requirements.

Assessment Methods And Objects

Examine: At a minimum, documentation for record retention audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements are met.

SI-12(FIS-1) – Enhancement (Moderate)

Control

Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design by a data processing control group, or some alternative. A data processing control group: (1) has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; (2) reviews output products for general acceptability; and (3) reconciles control information to determine completeness of processing.

Applicability: All	**References:** FISCAM: TAY-4.1.1, TAY-4.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12(FIS-1).1

Assessment Objective

Determine if the organization assigns responsibility for seeing that all outputs are produced and distributed according to system requirements and design by a data processing control group, or some alternative. A data processing control group: (1) has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; (2) reviews output products for general acceptability; and (3) reconciles control information to determine completeness of processing.

Assessment Methods And Objects

Examine: Output production and distribution.

Examine: Pertinent policies and procedures.

Interview: Information system and user management.

SI-12(FIS-2) – Enhancement (Moderate)

Control

Printed reports contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message.

Applicability: All	**References:** FISCAM: TAY-4.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12(FIS-2).1

Assessment Objective

Determine if the organizational information system printed reports contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message.

Assessment Methods And Objects

Examine: Application documentation.

Examine: Printed reports.

Interview: User personnel and application programmer, if available.

SI-12(FIS-3) – Enhancement (Moderate)

Control

Each output produced, whether printed or transmitted to a user's terminal device, is logged, manually if not automatically, including the recipient(s) who receive the output.

Applicability: All	**References:** FISCAM: TAY-4.1.4, TAY-4.1.5	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12(FIS-3).1

Assessment Objective

Determine if the organizational information system's output produced, whether printed or transmitted to a user's terminal device, is logged, manually if not automatically, including the recipient(s) who receive the output.

Assessment Methods And Objects

Examine: Application documentation.

Examine: Output logs.

Interview: Information system and user personnel.

SI-12(FIS-4) – Enhancement (Moderate)

Control

In the user department, outputs transmitted are summarized daily and printed for each terminal device, and reviewed by supervisors. A control log of output product errors is maintained, including the corrective actions take.

Applicability: All	**References:** FISCAM: TAY-4.1.7, TAY-4.1.8	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12(FIS-4).1

Assessment Objective

Determine if the organizational information system's user department, outputs transmitted are summarized daily and printed for each terminal device, and reviewed by supervisors. A control log of output product errors is maintained, including the corrective actions take.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Supporting documentation (e.g., printed daily summaries with supervisory initials or signatures).
Examine: This activity.
Interview: User supervisory personal.

SI-12(FIS-5) – Enhancement (Moderate)

Control

Users review output reports for data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction reports, (3) master record change reports, (4) exception reports, and (5) control totals balance reports. Output from reruns is subjected to the same quality review as the original output.

Applicability: All	**References:** FISCAM: TAY-4.1.9, TAY-4.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12(FIS-5).1

Assessment Objective

Determine if the organizational users review output reports for data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction reports, (3) master record change reports, (4) exception reports, and (5) control totals balance reports. Output from reruns is subjected to the same quality review as the original output.

Assessment Methods And Objects

Examine: Activity to review output reports.
Examine: Output reports.
Examine: Pertinent policies and procedures.
Interview: User management and personnel.

Business Partners Systems Security Manual

Appendix A, Attachment 3

CMS Core Security Requirements (CSR)

for

Low Impact Level Assessments

CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

Rev. 9

(This page intentionally left blank)

Access Control (AC) – *Technical*

AC-1 – Access Control Policy and Procedures (Low)

Control

Logical access controls and procedures shall be established and implemented effectively to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (i.e., programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

Guidance

The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AC-1; FISCAM: TAC-3.2.C.1, TAC-4.3.4, TSD-1.1.1, TSD-2.1, TSS-1.1.1; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1; NIST 800-53/53A: AC-1; PISP: 4.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents access control policy and procedures;
(ii) the organization disseminates access control policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review access control policy and procedures; and
(iv) the organization updates access control policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.
Interview: Organizational personnel with access control responsibilities.(Optional)

ASSESSMENT PROCEDURE: AC-1.2

Assessment Objective

Determine if:
(i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.
Interview: Organizational personnel with access control responsibilities.(Optional)

AC-1(FIS-1) – Enhancement (Low)

Control

Standard forms are used to document approval for archiving, deleting, or sharing data files. Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

Applicability: All	**References:** FISCAM: TAC-2.3.1, TAC-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-1(FIS-1).1

Assessment Objective

Determine if:
(i) the organization uses standard forms to document approval for archiving, deleting, or sharing data files; and
(ii) the organizational agreements, with other entities, document prior to sharing data or programs how the data files are protected.

Assessment Methods And Objects

Examine: Documents authorizing file sharing and file sharing agreements.
Examine: Pertinent policies and procedures.
Examine: Standard approval forms.
Interview: Data owners.

AC-2 – Account Management (Low)

Control

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. Access to the CMS information system shall be granted based on: (a) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (b) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

Guidance

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

Applicability: All	**References:** ARS: AC-2; FISCAM: TAC-3.2.C.4, TAC-3.2.C.5, TSP-4.1.6, TSS-1.1.3; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2.1

Assessment Objective

Determine if:
(i) the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts;
(ii) the organization defines the frequency of information system account reviews;
(iii) the organization reviews information system accounts at the organization-defined frequency, at least annually; and
(iv) the organization initiates required actions on information system accounts based on the review.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing account management; information system security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.
Interview: Organizational personnel with account management responsibilities.(Optional)

AC-2(0) – Enhancement (Low)

Control

Review information system accounts every 365 days and require annual certification.

Applicability: All	**References:** ARS: AC-2(0); FISCAM: TAC-3.2.C.4, TSS-1.1.4; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records.
Interview: Organizational personnel with account management responsibilities.(Optional)

AC-2(CMS-1) – Enhancement (Low)

Control

Remove or disable default user accounts. Rename active default accounts.

Applicability: All	**References:** ARS: AC-2(CMS-1); FISCAM: TAC-3.2.A.3, TAC-3.2.C.4, TSS-1.2.3; IRS-1075:	**Related Controls:**

	5.6.3.2#2.1	
ASSESSMENT PROCEDURE: AC-2(CMS-1).1		
Assessment Objective Determine if the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. **Assessment Methods And Objects** **Examine:** Access control policy and procedures; other relevant documents or records to determine if the organization removes or disables default user accounts. It must also rename active default accounts if they must be used. **Interview:** Organizational personnel with access control responsibilities to determine that all default user accounts are either removed or disabled. If default accounts are active, that they are renamed.		
AC-2(CMS-2) – Enhancement (Low)		
Control Require the use of unique and separate administrator accounts for administrator and non-administrator activities.		
Applicability: All	**References:** ARS: AC-2(CMS-2); FISCAM: TAN-2.1.4; IRS-1075: 5.6.3.2#2.1	**Related Controls:** IA-4(CMS-1)
ASSESSMENT PROCEDURE: AC-2(CMS-2).1		
Assessment Objective Determine if the information system enforces separation of duties through assigned access authorizations. **Assessment Methods And Objects** **Examine:** Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if the organization prohibits administrator accounts to be used for day-to-day activities. **Interview:** Organizational personnel with account management responsibilities to determine if administrator accounts are being used for day to day activities.		
AC-2(CMS-3) – Enhancement (Low)		
Control Implement centralized control of user access administrator functions.		
Applicability: All	**References:** ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(CMS-3).1		
Assessment Objective Determine if the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. **Assessment Methods And Objects** **Examine:** Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if all user access administrator functions are centralized. **Interview:** Organizational personnel with account management responsibilities to determine if all user access administrator functions are carried out by a centralized administrator function.		
AC-2(CMS-4) – Enhancement (Low)		
Control Regulate the access provided to contractors and define security requirements for contractors.		
Applicability: All	**References:** ARS: AC-2(CMS-4); IRS-1075: 5.6.3.2#2.1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(CMS-4).1		
Assessment Objective Determine if the organization documents contractor security requirements and maintains contractor access privileges. **Assessment Methods And Objects** **Examine:** Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if all contractors' access are authorized, regulated, and security requirements for contractors are defined. **Interview:** Organizational personnel with account management responsibilities to determine if written authorizations exist for a sample of contractor employees.		

AC-2(CMS-5) – Enhancement (Low)		
Control Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination.		
Applicability: All	**References:** ARS: AC-2(CMS-5); FISCAM: TSP-4.1.6; IRS-1075: 5.6.3.2#2.1	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(CMS-5).1		
Assessment Objective Determine if the organization terminates information system access upon termination of individual employment. **Assessment Methods And Objects** **Examine:** Access control policy; account management procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine when employee access rights are revoked on termination. **Interview:** Organizational personnel with personnel security responsibilities to determine when access is revoked on employee termination.		
AC-2(FIS-1) – Enhancement (Low)		
Control All system access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to security managers.		
Guidance The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties.		
Applicability: All	**References:** FISCAM: TAC-2.1.1, TAC-2.2	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(FIS-1).1		
Assessment Objective Determine if: (i) the organization grants system access authorizations on standard forms and maintains the completed forms on file; and (ii) the organizational senior managers approve system access authorizations and the approvals are securely transferred to security managers. **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Selection of user (both application user and information system personnel) access authorization documentation. **Interview:** Personnel involved in access authorizations and senior managers who approve authorizations.		
AC-2(FIS-2) – Enhancement (Low)		
Control Business Owners periodically review system access authorization listings and determine whether they remain appropriate. ISSO/SSOs review system access authorizations and discuss any questionable authorizations with Business Owners.		
Applicability: All	**References:** FISCAM: TAC-2.1.2, TAC-2.1.4	**Related Controls:**
ASSESSMENT PROCEDURE: AC-2(FIS-2).1		
Assessment Objective Determine if the organization security managers periodically reviews system access authorization listings and discusses questionable authorizations with management. **Assessment Methods And Objects** **Examine:** Access authorization listings to determine whether inappropriate access are removed in a timely manner. **Examine:** Pertinent policies and procedures. **Interview:** Business Owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner. **Interview:** Security managers and review documentation provided to them.		
AC-2(3) – Enhancement (Low)		
Control Configure the information system to disable inactive accounts automatically after 365 days.		
Applicability: All	**References:**	**Related Controls:** IA-4(0)

ASSESSMENT PROCEDURE: AC-2(3).1

Assessment Objective

Determine if:
(i) the organization defines a time period after which the information system disables inactive accounts; and
(ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.

Assessment Methods And Objects

Examine: Procedures addressing account management; information system security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing account management functions.(Optional)

AC-3 – Access Enforcement (Low)

Control

Access enforcement mechanisms shall be developed, documented and implemented effectively to control access between named users (or processes) and named objects (e.g., files and programs) in a CMS information system. Additional application level access enforcement mechanism shall be implemented, when necessary, to provide increased information security for CMS information. When encryption of stored information is employed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (see section 4.16.13).

Guidance

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

Applicability: All	**References:** ARS: AC-3; FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.C.6, TAC-3.2.D.1, TCC-3.2.3, TSS-2.1.1, TSS-2.1.2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3; NIST 800-53/53A: AC-3; PISP: 4.1.3	**Related Controls:** MA-CMS-1, MA-CMS-2, SC-13

ASSESSMENT PROCEDURE: AC-3.1

Assessment Objective

Determine if:
(i) the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy; and
(ii) user privileges on the information system are consistent with the documented user authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing access enforcement policy.(Optional)

AC-3(1) – Enhancement (Low)

Control

Ensure the information system restricts access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.

Guidance

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Applicability: All	**References:** ARS: AC-3(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.2, TAC-3.2.C.5, TAC-3.2.D.1, TCC-3.2.3, TSD-3.1.4, TSS-1.1.2, TSS-2.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-3(1).1

Assessment Objective

Determine if:
(i) the organization explicitly defines privileged functions and security-relevant information for the information system;
(ii) the organization explicitly authorizes personnel access to privileged functions and security-relevant information in accordance with organizational policy; and
(iii) the information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel (e.g., security administrators).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing access enforcement policy.(Optional)

AC-3(CMS-1) – Enhancement (Low)

Control

If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Applicability: All	**References:** ARS: AC-3(CMS-1)	**Related Controls:** SC-13

ASSESSMENT PROCEDURE: AC-3(CMS-1).1

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if encryption is used as an access control mechanism, examine system and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Interview: Organizational personnel with access control responsibilities to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

AC-3(CMS-2) – Enhancement (Low)

Control

If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix A for e-Authentication Standards.

Applicability: All	**References:** ARS: AC-3(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-3(CMS-2).1

Assessment Objective

Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if e-authentication is used as an access control mechanism, examine Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the organization's encryption standard meets ARS Appendix A for e-Authentication Standards.

Interview: Organizational personnel with access control responsibilities if e-authentication is used as an access control mechanism, interview system administrators responsible for the hosts providing authentication services to determine if the organization meets the standards described in ARS Appendix A.

AC-3(CMS-3) – Enhancement (Low)

Control

Configure operating system controls to disable public "write" access to files, objects, and directories that may directly impact system functionality and/or performance.

Applicability: All	**References:** ARS: AC-3(CMS-3); FISCAM: TAC-3.2.D.1, TCC-3.2.3; IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-3(CMS-3).1

Assessment Objective

Determine if the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

Interview: Organizational personnel with access control responsibilities to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

AC-5 – Separation of Duties (Low)

Control

The principle of separation of duties shall be enforced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission functions and distinct information systems support functions shall be divided among different roles, and support functions shall be performed by different individuals (e.g., personnel responsible for administering access control functions shall not also administer audit functions). Personnel developing and testing system code shall not have access to production libraries. Access control software shall be in place to limit individual authority and information access, such that the collusion of two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties.

Guidance

The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Applicability: All	References: ARS: AC-5; FISCAM: TAY-1.3.2, TSD-1.1.1, TSD-1.1.2, TSD-1.1.3, TSD-1.1.5, TSD-1.2.1, TSD-1.3.3, TSD-2.2.2, TSS-1.1.2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3; NIST 800-53/53A: AC-5; PISP: 4.1.5	Related Controls:

ASSESSMENT PROCEDURE: AC-5.1

Assessment Objective

Determine if:
(i) the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and
(ii) the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing separation of duties; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records.(Optional)
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties.(Optional)
Test: Automated mechanisms implementing separation of duties policy.(Optional)

AC-5(CMS-1) – Enhancement (Low)

Control

Ensure that audit functions are not performed by security personnel responsible for administering access control.

Applicability: All	References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5	Related Controls:

ASSESSMENT PROCEDURE: AC-5(CMS-1).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if audit functions are NOT performed by security personnel responsible for administering access control. Also, ensure that the organization enforces separation of duties through assigned access authorizations.
Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are NOT performed by security personnel. Also, determine if access authorizations complement and reinforce separation of duties.

AC-5(CMS-2) – Enhancement (Low)

Control

Maintain a limited group of administrators with access based upon the users' roles and responsibilities.

Applicability: All	References: ARS: AC-5(CMS-2)	Related Controls:

ASSESSMENT PROCEDURE: AC-5(CMS-2).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization maintains a limited group of administrators with access based upon the users' roles and responsibilities.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the number of personnel with root access is limited to only those personnel with a business need for root access.

AC-5(CMS-3) – Enhancement (Low)

Control

Ensure that critical mission functions and information system support functions are divided among separate individuals.

Applicability: All	**References:** ARS: AC-5(CMS-3); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-3).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals.

AC-5(CMS-4) – Enhancement (Low)

Control

Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Applicability: All	**References:** ARS: AC-5(CMS-4); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(CMS-4).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

AC-5(FIS-1) – Enhancement (Low)

Control

Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.

Applicability: All	**References:** FISCAM: TSD-1.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-5(FIS-1).1

Assessment Objective

Determine if the organization provides adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Interview: Personnel to determine whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.

AC-6 – Least Privilege (Low)

Control

Each user or process shall be assigned the most restrictive set of privileges needed for the performance of authorized tasks.

Guidance

The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Applicability: All	**References:** ARS: AC-6; FISCAM: TSD-2.1; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); HSPD 7: D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2; NIST 800-53/53A: AC-6; PISP: 4.1.6	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6.1

Assessment Objective

Determine if:
(i) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks; and
(ii) the information system enforces the most restrictive set of rights/privileges or accesses needed by users.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.(Optional)
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.(Optional)

AC-6(CMS-1) – Enhancement (Low)

Control

Disable all file system access not explicitly required for system, application, and administrator functionality.

Applicability: All	**References:** ARS: AC-6(CMS-1); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6(CMS-1).1

Assessment Objective

Determine if the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if all file system access not explicitly required for system, application, and administrator functionality is disabled.
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine hosts that store, transmit or process sensitive data to determine if file system access not explicitly required for system, application, and administrator functionality are disabled.

AC-6(CMS-2) – Enhancement (Low)

Control

Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.

Applicability: All	**References:** ARS: AC-6(CMS-2); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6(CMS-2).1

Assessment Objective

Determine if the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if contractors are required to be provided with minimal system and physical access, and that they've agreed to support the CMS security requirements. The documented contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine the default access levels given to contractors. Ensure that all file system access not explicitly required for system, application, and administrator functionality is disabled.

AC-6(CMS-3) – Enhancement (Low)

Control

Restrict the use of database management utilities to only authorized database administrators.

Applicability: All	**References:** ARS: AC-6(CMS-3); FISCAM: TAC-3.2.D.1, TAC-3.2.D.2, TAC-3.2.D.3, TAC-3.2.D.4	**Related Controls:**

ASSESSMENT PROCEDURE: AC-6(CMS-3).1

Assessment Objective

Determine if the information system enforces separation of duties through assigned access authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system restricts the use of database management utilities to only authorized database administrators. Policies and procedures must also prevent users from accessing database data files at the logical data view, field, or field-value levels. Implement column-level access controls.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine if the information system restricts the use of database management utilities to only authorized database administrators. Also, determine whether or not users are prevented from accessing database data files at the logical data view, field, or field-value levels. Column-level access controls must also be implemented.

AC-7 – Unsuccessful Log-on Attempts (Low)

Control

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce a limit of CMS-defined consecutive invalid access attempts by a user during a specified time period. Systems shall be locked after a specified number of multiple unsuccessful log-on attempts.

Guidance

Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Applicability: All	**References:** ARS: AC-7; IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7	**Related Controls:**

ASSESSMENT PROCEDURE: AC-7.1

Assessment Objective

Determine if:

(i) the organization defines the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur;

(ii) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period;

(iii) the organization defines the time period for lock out mode or delay period;

(iv) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; and

(v) the information system enforces the organization-selected lock out mode or delayed login prompt.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing unsuccessful logon attempts; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts.(Optional)

AC-7(0) – Enhancement (Low)

Control

Configure the information system to disable access for at least five (5) minutes after three (3) failed log-on attempts by a user during a five (5) minute time period.

Applicability: All	**References:** ARS: AC-7(0); IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7	**Related Controls:** AC-9

ASSESSMENT PROCEDURE: AC-7(0).1

Assessment Objective

Determine if the organization configures system lockout to assist in preventing password guessing.

Assessment Methods And Objects

Examine: Password lockout policy includes failed log-on attempts, lockout timeframes period for failed attempts and system/network administrator account reset capabilities.

Interview: A sampling of users for knowledge of log-on and account lockout procedure policy is known.

AC-8 – System Use Notification (Low)

Control

An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security

notices (based on associated privacy and security policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS information system.

Guidance

Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Applicability: All	**References:** ARS: AC-8; FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2; NIST 800-53/53A: AC-8; PISP: 4.1.8	**Related Controls:** SI-4

ASSESSMENT PROCEDURE: AC-8.1

Assessment Objective

Determine if:
(i) the information system displays a system use notification message before granting system access informing potential users:
- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording;

(ii) the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).
(iii) the organization approves the information system use notification message before its use; and
(iv) the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for system use notification.(Optional)

AC-8(CMS-1) – Enhancement (Low)

Control

Configure the information system to display a warning banner automatically prior to granting access to potential users. Notify users that:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.

Guidance

All CMS information system computers and network devices under their control, independently, prominently and completely display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web, ftp, telnet, or other services accessed.

Applicability: All	**References:** ARS: AC-8(CMS-1); FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-1).1

Assessment Objective

Determine if the information system displays a system use notification message before granting system access informing potential users:
- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if the information system is configured to display a warning banner automatically prior to granting access to potential users. Notify users that:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;

(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.
Interview: Organizational personnel to determine if hosts are configured to present a warning banner at system access points. The warning banner must contain the following elements:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;
(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.

AC-8(CMS-2) – Enhancement (Low)

Control

Develop and implement the warning banner in conjunction with legal counsel.

Applicability: All	**References:** ARS: AC-8(CMS-2); IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-2).1

Assessment Objective

Determine if the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if warning banners were developed and implemented in conjunction with legal counsel.
Interview: Organizational personnel to determine if warning banners were developed and implemented in conjunction with legal counsel.

AC-8(CMS-3) – Enhancement (Low)

Control

Post clear privacy policies on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.

Applicability: All	**References:** ARS: AC-8(CMS-3); IRS-1075: 5.6.3.2#4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-8(CMS-3).1

Assessment Objective

Determine if the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if clear privacy policies are posted on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.
Interview: Organizational personnel to determine if clear privacy policies are posted where substantial personal information from the public is collected.

AC-13 – Supervision and Review—Access Control (Low)

Control

Personnel shall be supervised and reviewed with respect to the usage of CMS information system access controls. Automated mechanisms shall be in place to facilitate the review of audit records, and any unusual activities shall be investigated in a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of users with significant information system roles and responsibilities shall be reviewed more frequently.

Guidance

The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**References:** ARS: AC-13; FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSD-3.2.1, TSD-3.2.3, TSS-2.1.3; HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: AC-13; PISP: 4.1.13	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13.1

Assessment Objective

Determine if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records.

Interview: Organizational personnel with supervisory and access control responsibilities.(Optional)

AC-13(CMS-1) – Enhancement (Low)

Control

Review integrity of files and directories for unexpected and/or unauthorized changes at least once per day. Automate the review of file creation, changes and deletions; and monitor permission changes. Generate alert notification for technical staff review and assessment.

Applicability: All	**References:** ARS: AC-13(CMS-1); FISCAM: TAC-2.1.5; HIPAA: 164.312(c)(2), 164.312(e)(2)(i)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(CMS-1).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records to determine if files and directories are reviewed for unexpected and/or unauthorized changes at least once per day. The review of file creation, changes and deletions, and permission changes must be monitored automatically. Alert notifications must be generated for technical staff review and assessment.

Interview: Organizational personnel with supervisory and access control responsibilities to determine if the integrity of files and directories for unexpected and/or unauthorized changes at least once per day. Determine if file creation, changes and deletions, and permission changes are being reviewed automatically. Determine if alert notifications for technical staff review and assessment are being generated.

AC-13(CMS-2) – Enhancement (Low)

Control

Enable logging of administrator and user account activities, system shutdowns, reboots, errors and access authorizations.

Applicability: All	**References:** ARS: AC-13(CMS-2); FISCAM: TAC-2.1.5, TAN-2.1.8, TSS-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(CMS-2).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records to determine if logging of administrator and user account activities, system shutdowns, reboots, errors and access authorizations is enabled.

Interview: Organizational personnel with supervisory and access control responsibilities to determine if logging of administrator and user account activities, system shutdowns, reboots, errors and access authorizations is enabled.

AC-13(CMS-3) – Enhancement (Low)

Control

Inspect administrator groups, root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that unauthorized accounts have not been created.

Applicability: All	**References:** ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(CMS-3).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system related accounts are inspected on demand, but at least once every thirty (30) days to ensure that unauthorized accounts have not been created.

Interview: Organizational personnel with supervisory and access control responsibilities to determine if administrator groups, root accounts and other system related accounts are inspected on

demand, but at least once every thirty (30) days to ensure that unauthorized accounts have not been created.

AC-13(FIS-1) – Enhancement (Low)

Control

Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

Applicability: All	**References:** FISCAM: TSD-1.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: AC-13(FIS-1).1

Assessment Objective

Determine if the organizational supervisory personnel review transactions performed.

Assessment Methods And Objects

Examine: Activities and test transaction reviews.
Examine: Pertinent policies and procedures.
Interview: Management.

AC-14 – Permitted Actions without Identification or Authentication (Low)

Control

Based upon mission / business requirements, public access to CMS information systems without identification and authorization shall be limited to public websites and other publicly available systems. CMS information systems shall be configured to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

Guidance

The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov).

Applicability: All	**References:** ARS: AC-14; NIST 800-53/53A: AC-14; PISP: 4.1.14	**Related Controls:** IA-2

ASSESSMENT PROCEDURE: AC-14.1

Assessment Objective

Determine if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for permitted actions without identification and authentication.(Optional)

AC-16 – Automated Labeling (Low)

Control

CMS information systems shall label information “in storage,” “in process,” and “in transit” with special dissemination handling or distribution instructions, in a manner consistent with this policy.

Guidance

Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.

Applicability: All	**References:** ARS: AC-16; NIST 800-53/53A: AC-16; PISP: 4.1.16	**Related Controls:** AC-15

ASSESSMENT PROCEDURE: AC-16.1

Assessment Objective

Determine if the information system appropriately labels information in storage, in process, and in transmission.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Automated mechanisms implementing automated (internal) labeling within the information system.(Optional)

AC-16(CMS-1) – Enhancement (Low)

Control

If automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

Applicability: All	**References:** ARS: AC-16(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-16(CMS-1).1

Assessment Objective

Determine if the information system appropriately labels information in storage, in process, and in transmission.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine, if automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

Interview: Organization personnel to determine, if automated information labeling is utilized, that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

AC-17 – Remote Access (Low)

Control

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can access the information system from remote locations shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, shall not be used to gain access to a CMS information system that processes CMS sensitive information unless the CIO or his/her designated representative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-up capabilities.

Guidance

Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST SP 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 and 800-78. NIST SP 800-77 provides guidance on IPSec-based virtual private networks.

Applicability: All	**References:** ARS: AC-17; FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17; PISP: 4.1.17	**Related Controls:** IA-2, SC-9

ASSESSMENT PROCEDURE: AC-17.1

Assessment Objective

Determine if the organization documents, monitors, and controls all methods of remote access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities.(Optional)

AC-17(4) – Enhancement (Low)

Control

Permit remote access for privileged functions only for compelling operational needs and document the rationale for such access in the security plan for the information system.

Applicability: All	**References:** ARS: AC-17(4); FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(4).1

Assessment Objective

Determine if:

(i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed; and

(ii) the organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing the access control policy for remote access.(Optional)

AC-17(CMS-1) – Enhancement (Low)		
Control Enable secure management protocols through a VPN link(s) if connected to the information system and using remote administration.		
Applicability: All	**References:** ARS: AC-17(CMS-1); IRS-1075: 5.6.3.2#5	**Related Controls:** SC-13
ASSESSMENT PROCEDURE: AC-17(CMS-1).1		
Assessment Objective Determine if the organization documents, monitors, and controls all methods of remote access to the information system. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if secure management protocols through a VPN link(s) if connected to the information system and using remote administration are enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system. **Interview:** Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if secure management protocols through a VPN link(s) if connected to the information system and using remote administration are enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system.		
AC-17(CMS-2) – Enhancement (Low)		
Control Implement password protection for remote access connections.		
Applicability: All	**References:** ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5	**Related Controls:**
ASSESSMENT PROCEDURE: AC-17(CMS-2).1		
Assessment Objective Determine if the organization documents, monitors, and controls all methods of remote access to the information system. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if password protection for remote access connections is implemented. **Interview:** Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if password protection is required for remote access connections.		
AC-17(CMS-3) – Enhancement (Low)		
Control Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) cannot be used.		
Applicability: All	**References:** ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	**Related Controls:**
ASSESSMENT PROCEDURE: AC-17(CMS-3).1		
Assessment Objective Determine if: (i) the organization defines managed access control points for remote access to the information system; and (ii) the information system controls all remote accesses through a limited number of managed access control points. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified annually. **Interview:** Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually.		
AC-17(CMS-4) – Enhancement (Low)		
Control If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix A for e-Authentication standards.		
Applicability: All	**References:** ARS: AC-17(CMS-4); IRS-1075: 5.6.3.2#5	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(CMS-4).1

Assessment Objective

Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if e-authentication is implemented as a remote access solution or associated with remote access. If so, refer to ARS Appendix A for e-Authentication standards.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system implements e-authentication. If so, refer to ARS Appendix A for e-Authentication standards.

AC-17(FIS-1) – Enhancement (Low)

Control

Remote access phone numbers are not published and are periodically changed.

Applicability: All	**References:** FISCAM: TAC-3.2.E.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AC-17(FIS-1).1

Assessment Objective

Determine if the organization changes, periodically, remote access phone numbers and those phone numbers are not published.

Assessment Methods And Objects

Examine: Documentation showing changes to dial-in numbers.

Examine: Entity's telephone directory to verify that the numbers are not listed.

Examine: Pertinent policies and procedures.

Interview: Remote access users.

AC-18 – Wireless Access Restrictions (Low)

Control

Installation of wireless access points (WAP) into CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. Authorized WAP devices and wireless access shall be monitored on a regular basis, and wireless communications shall be secured through the use of approved encryption controls.

Guidance

NIST SP 800-48 and 800-97 provide guidance on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion detection and prevention.

Applicability: All	**References:** ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18	**Related Controls:**

ASSESSMENT PROCEDURE: AC-18.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for wireless technologies;
(ii) the organization authorizes, monitors, and controls wireless access to the information system; and
(iii) the wireless access restrictions are consistent with NIST SP 800-48 and 800-97.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records.

Test: Wireless access usage and restrictions.(Optional)

AC-18(0) – Enhancement (Low)

Control

CMS policy prohibits the use of wireless access unless explicitly approved by the CMS CIO or his/her designated representative.

Applicability: All	**References:** ARS: AC-18(0); NIST 800-53/53A: AC-18; PISP: 4.1.18	**Related Controls:**

ASSESSMENT PROCEDURE: AC-18(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records.

AC-18(DIR-1) – Enhancement (Low)

Control

If wireless access is explicitly approved, wireless devices, service set identifier broadcasting is disabled and the following wireless access controls are implemented:
(a) encryption protection is enabled;
(b) access points are placed in secure areas;
(c) access points are shut down when not in use (i.e., nights, weekends);
(d) a firewall is implemented between the wireless network and the wired infrastructure;
(e) MAC address authentication is utilized;
(f) static IP addresses, not DHCP, is utilized;
(g) personal firewalls are utilized on all wireless clients;
(h) file sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall; and
(j) wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

Applicability: All	**References:**	**Related Controls:**

ASSESSMENT PROCEDURE: AC-18(DIR-1).1

Assessment Objective

Determine if the organization establishes wireless policies and strict procedures that control access to the wireless LAN and separates/restricts the wireless LAN from the wired network infrastructure.

Assessment Methods And Objects

Examine: Access control procedures for continuous wireless intrusion monitoring of approved and operational wireless systems.

Interview: Staff personnel who review the wireless LAN records know what to look for in the data for an unauthorized intrusion, and the staff knows the reporting procedures when an unauthorized intrusion is detected.

AC-19 – Access Control for Portable and Mobile Devices (Low)

Control

The connection of portable and mobile devices (e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CIO or his/her designated representative. Prior to connecting portable and mobile devices to CMS information systems and networks, such devices shall be configured to comply with CMS IS policies and procedures. The storage and transmission of CMS sensitive information on portable and mobile information devices shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware. The activities and controls shall be commensurate with the system security level of the information.

Guidance

Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family.

Applicability: All	**References:** ARS: AC-19; IRS-1075: 4.6#1; NIST 800-53/53A: AC-19; PISP: 4.1.19	**Related Controls:** MP-4, MP-5

ASSESSMENT PROCEDURE: AC-19.1

Assessment Objective

Determine if:
(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;
(ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and
(iii) the organization authorizes, monitors, and controls device access to organizational information systems.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.(Optional)

Interview: Organizational personnel who use portable and mobile devices to access the information system.(Optional)

Test: Automated mechanisms implementing access control policy for portable and mobile devices.(Optional)

AC-20 – Use of External Information Systems (Low)

Control

External information systems, including, but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports shall not be used to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative.

Strict terms and conditions shall be established for the use of external information systems. The terms and conditions shall address, at a minimum:
4.1.20.1. The types of applications that can be accessed from external information systems;
4.1.20.2. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
4.1.20.3. How other users of the external information system will be prevented from accessing federal information;
4.1.20.4. The use of virtual private networking (VPN) and firewall technologies;
4.1.20.5. The use of and protection against the vulnerabilities of wireless technologies;
4.1.20.6. The maintenance of adequate physical security controls;
4.1.20.7. The use of virus and spyware protection software; and
4.1.20.8. How often the security capabilities of installed software are to be updated.

Guidance

External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.
Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Applicability: All	**References:** ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20	**Related Controls:**

ASSESSMENT PROCEDURE: AC-20.1

Assessment Objective

Determine if:
(i) the organization defines the types of applications that can be accessed from the external information system;
(ii) the organization defines the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system; and
(iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel who use external information systems to access the information system.(Optional)

AC-20(CMS-1) – Enhancement (Low)

Control

Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.

Applicability: All	**References:** ARS: AC-20(CMS-1); IRS-1075: 4.7.2#1, 4.7.3#3	**Related Controls:**

ASSESSMENT PROCEDURE: AC-20(CMS-1).1

Assessment Objective

Determine if the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

Interview: Organizational personnel who use external information systems to access the information system to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

AC-CMS-1 – System Boot Access (Low)

Control

System boot access shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can alter or perform non-standard boots of systems and/or components of the information system shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Guidance

When a person has unrestrained physical access to any computing system or network device the person has control of the equipment.
If the person does not have the capability to locally access the information system's data though the boot process this can assist in protecting the data from loss or unauthorized access to the data.
Note: Even though the system root access may be protected by privilege access controls a miss configured system can allow the system to reboot and thus allowing a boot / access from unauthorized media. An example of this is a LINUX system, not configured correctly, when CONT+ALT+DEL is issued from the keyboard the equipment will re-boot automatically.

Applicability: All	**References:** ARS: AC-CMS-1; PISP: 4.1.21	**Related Controls:**

ASSESSMENT PROCEDURE: AC-CMS-1.1

Assessment Objective

Determine if the organization assesses the need for system boot access and if necessary controls, documents and monitors the continued need for system boot access.

Assessment Methods And Objects

Examine: System boot access documentation to determine that there is or is not a need for boot access.

Interview: Organizational personnel to determine that there is or is not a need for system boot access.

AC-CMS-1(CMS-1) – Enhancement (Low)

Control

If not explicitly required, boot access to removable media drives is disabled.

Applicability: All	**References:** ARS: AC-CMS-1(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: AC-CMS-1(CMS-1).1

Assessment Objective

Determine if the organization evaluates the need for system boot access by removable media drives.

Assessment Methods And Objects

Examine: System boot access documentation to determine that, if not explicitly required, boot access to removable media drives is disabled.

Interview: Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled.

AC-CMS-1(CMS-2) – Enhancement (Low)

Control

System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).

Applicability: All	**References:** ARS: AC-CMS-1(CMS-2)	**Related Controls:** IA-5

ASSESSMENT PROCEDURE: AC-CMS-1(CMS-2).1

Assessment Objective

Determine if the organization controls access to the system BIOS when unauthorized personnel may be in physical proximity to the system.

Assessment Methods And Objects

Examine: System BIOS documentation to determine if System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).

Interview: Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled.

Awareness and Training (AT) – *Operational*

AT-1 – Security Awareness and Training Policy and Procedures (Low)

Control

An IS AT program shall be developed, documented, and implemented effectively for all personnel, including contractors and any other users of CMS information and information systems. The IS AT program shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information, information systems, and networks.

Guidance

The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-16 and 800-50 provide guidance on security awareness and training. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AT-1; FISCAM: TSP-4.2.2; IRS-1075: 5.6.2.7#1.1-2, 6.1#1; NIST 800-53/53A: AT-1; PISP: 4.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: AT-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security awareness and training policy and procedures;
(ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review security awareness and training policy and procedures; and
(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.
Interview: Organizational personnel with security awareness and training responsibilities.(Optional)

ASSESSMENT PROCEDURE: AT-1.2

Assessment Objective

Determine if:
(i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.
Interview: Organizational personnel with security awareness and training responsibilities.(Optional)

AT-2 – Security Awareness (Low)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS AT program shall be consistent with 5 CFR Part 930 (http://opm.gov/fedregis/2004/69-061404-32835-a.pdf) and the guidance provided in NIST SP 800-50.

Guidance

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	**References:** ARS: AT-2; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3; NIST 800-53/53A: AT-2; PISP: 4.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2.1

Assessment Objective

Determine if:

(i) the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes;
(ii) the security awareness training is consistent with applicable regulations and NIST SP 800-50;
(iii) the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access;
(iv) the organization defines the frequency of refresher security awareness training; and
(v) the organization provides refresher security awareness training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan; other relevant documents or records.
Interview: Organizational personnel comprising the general information system user community.(Optional)

AT-2(0) – Enhancement (Low)

Control

All information system users (including managers and senior executives) receive basic information security awareness training prior to accessing any system's information; when required by system changes; and every 365 days thereafter.

Applicability: All	**References:** ARS: AT-2(0); FISCAM: TSP-3.3.1; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3, 6.2#1.1-2, 6.2#1.4, 6.2#2.1; NIST 800-53/53A: AT-2; PISP: 4.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan (for organization-defined frequency of refresher security awareness training); other relevant documents or records.

AT-2(CMS-1) – Enhancement (Low)

Control

Establish a program to promote continuing awareness of information security issues and threats.

Applicability: All	**References:** ARS: AT-2(CMS-1); HIPAA: 164.308(a)(5)(ii)(A); IRS-1075: 5.6.2.7#1.3	**Related Controls:**

ASSESSMENT PROCEDURE: AT-2(CMS-1).1

Assessment Objective

Determine if the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records to determine that a program to promote continuing awareness of information security issues and threats has been established.
Interview: Organizational personnel with security awareness and training responsibilities to determine that a program to promote continuing awareness of information security issues and threats has been established.

AT-3 – Security Training (Low)

Control

The organization shall identify and document all positions and/or roles with significant information system security responsibilities during the system development life cycle. All personnel with significant information system security responsibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Content of the security awareness training shall be determined based upon the information systems to which personnel have authorized access. The employee shall acknowledge having received the security and awareness training either in writing or electronically as part of the training course completion.

Guidance

The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	**References:** ARS: AT-3; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: AT-3.1

Assessment Objective

Determine if:
(i) the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities;
(ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes;
(iii) the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security;
(iv) the security training is consistent with applicable regulations and NIST SP 800-50;
(v) the organization defines the frequency of refresher security training; and
(vi) the organization provides refresher security training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan; other relevant documents or records.
Interview: Organizational personnel with significant information system security responsibilities.(Optional)

AT-3(0) – Enhancement (Low)

Control

Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to CMS networks, systems, and/or applications; when required by system changes; and refresher training every 365 days thereafter.

Applicability: All	**References:** ARS: AT-3(0); FISCAM: TSP-3.3.1; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: AT-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan (for organization-defined frequency of refresher security training); other relevant documents or records.

AT-4 – Security Training Records (Low)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that individual IS training activities, including basic security awareness training and specific information system security training, are properly documented and monitored.

Guidance

Procedures and training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.
(2) Executives must receive training in information security basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	References: ARS: AT-4; FISCAM: TSP-4.2.3; IRS-1075: 6.2#1.3; NIST 800-53/53A: AT-4; PISP: 4.2.4	Related Controls:

ASSESSMENT PROCEDURE: AT-4.1

Assessment Objective

Determine if the organization monitors and documents basic security awareness training and specific information system security training.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.

AT-5 – Contacts with Security Groups and Associations (Low)

Control

Contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations shall be encouraged and supported to enable security personnel to stay up to date with the latest recommended security practices, techniques, and technologies; and to share the latest security-related information including threats, vulnerabilities, and incidents.

Guidance

To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Applicability: All	References: ARS: AT-5; HSPD 7: H(25); NIST 800-53/53A: AT-5; PISP: 4.2.5	Related Controls:

ASSESSMENT PROCEDURE: AT-5.1

Assessment Objective

Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security techniques and technologies and to share security-related information.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records.(Optional)

Audit and Accountability (AU) – *Technical*

AU-1 – Audit and Accountability Policy and Procedures (Low)

Control

All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the implementation and management of audit controls, and shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: AU-1; IRS-1075: 5.6.3.3#1; NIST 800-53/53A: AU-1; PISP: 4.3.1	**Related Controls:**

ASSESSMENT PROCEDURE: AU-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents audit and accountability policy and procedures;
(ii) the organization disseminates audit and accountability policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review audit and accountability policy and procedures; and
(iv) the organization updates audit and accountability policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Audit and accountability policy and procedures; other relevant documents or records.
Interview: Organizational personnel with audit and accountability responsibilities.(Optional)

ASSESSMENT PROCEDURE: AU-1.2

Assessment Objective

Determine if:
(i) the audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Audit and accountability policy and procedures; other relevant documents or records.
Interview: Organizational personnel with audit and accountability responsibilities.(Optional)

AU-2 – Auditable Events (Low)

Control

Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security incidents. The selection of auditable events shall be based upon a risk assessment as to which events require auditing on a continuous basis, and which events require auditing in response to specific situations.

Guidance

The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**References:** ARS: AU-2; FISCAM: TAC-4.3.4, TSD-3.2.2; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2; PISP: 4.3.2	**Related Controls:** AU-4

ASSESSMENT PROCEDURE: AU-2.1

Assessment Objective

Determine if:
(i) the organization defines information system auditable events;
(ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and
(iii) the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing information system auditing of organization-defined auditable events.(Optional)

AU-2(0) – Enhancement (Low)

Control

Generate audit records for the following events:
(a) User account management activities,
(b) System shutdown,
(c) System reboot,
(d) System errors,
(e) Application shutdown,
(f) Application restart,
(g) Application errors,
(h) File creation, and
(i) File deletion.

Applicability: All	**References:** ARS: AU-2(0); FISCAM: TAC-2.1.5, TAC-4.1, TSD-3.2.4; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3; NIST 800-53/53A: AU-2; PISP: 4.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AU-2(CMS-1) – Enhancement (Low)

Control

Enable logging for perimeter devices, including firewalls and routers.
(a) Log packet screening denials originating from untrusted networks,
(b) Packet screening denials originating from trusted networks,
(c) User account management,
(d) Modification of packet filters,
(e) Application errors,
(f) System shutdown and reboot, and
(g) System errors.

Applicability: All	**References:** ARS: AU-2(CMS-1); HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines information system auditable events;
(ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and
(iii) the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if logging-on is enabled for perimeter devices, including firewalls and routers. This logging will capture the following information:
(a) Log packet screening denials originating from un-trusted networks,
(b) packet screening denials originating from trusted networks,
(c) user account management,
(d) modification of proxy services,
(e) application errors,
(f) system shutdown and reboot,
(g) system errors,
(h) modification of proxy services, and
(i) modification of packet filters.

Interview: Organizational personnel with audit and accountability responsibilities to determine if logging-on is enabled for perimeter devices, including firewalls and routers. This logging will capture the following information:
(a) Log packet screening denials originating from un-trusted networks,
(b) packet screening denials originating from trusted networks,
(c) user account management,
(d) modification of proxy services,
(e) application errors,
(f) system shutdown and reboot,
(g) system errors,
(h) modification of proxy services, and
(i) modification of packet filters.

AU-2(CMS-2) – Enhancement (Low)

Control

Verify that proper logging is enabled in order to audit administrator activities.

Applicability: All	**References:** ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-2(CMS-2).1

Assessment Objective

Determine if the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if proper logging is enabled in order to audit administrator activities.

Interview: Organizational personnel with account audit and accountability responsibilities to determine if proper logging is enabled in order to audit administrator activities.

AU-3 – Content of Audit Records (Low)

Control

Automated mechanisms shall be established to provide the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome.

Guidance

Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**References:** ARS: AU-3; FISCAM: TAC-3.2.D.1, TAN-2.1.9; IRS-1075: 5.6.3.3#3; NIST 800-53/53A: AU-3; PISP: 4.3.3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-3.1

Assessment Objective

Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records.

Test: Automated mechanisms implementing information system auditing of auditable events.(Optional)

AU-4 – Audit Storage Capacity (Low)

Control

A sufficient amount of information system storage capacity shall be allocated for audit records, and information systems shall be configured to reduce the likelihood of audit records exceeding such storage capacity.

Guidance

The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements.

Applicability: All	**References:** ARS: AU-4; IRS-1075: 5.6.3.3#4; NIST 800-53/53A: AU-4; PISP: 4.3.4	**Related Controls:** AU-2, AU-5, AU-6, AU-7, SI-4

ASSESSMENT PROCEDURE: AU-4.1

Assessment Objective

Determine if:

(i) the organization defines audit record storage capacity for the information system components that generate audit records; and

(ii) the organization establishes information system configuration settings to reduce the likelihood of the audit record storage capacity being exceeded.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components generating audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AU-5 – Response to Audit Processing Failures (Low)

Control

Automated mechanisms shall be established which provide the capability to generate information system alerts for appropriate officials in the event of an audit failure or audit storage capacity being reached and to take appropriate additional actions.

Guidance

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Applicability: All	**References:** ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5	**Related Controls:** AU-4

ASSESSMENT PROCEDURE: AU-5.1

Assessment Objective

Determine if:

(i) the organization defines actions to be taken in the event of an audit processing failure;

(ii) the organization defines personnel to be notified in case of an audit processing failure; and

(iii) the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure or audit storage capacity being reached.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system response to audit processing failures.(Optional)

AU-5(0) – Enhancement (Low)

Control

Alert appropriate officials and take the following actions in response to an audit failure or audit storage capacity issue:

(a) Shutdown the information system,

(b) Stop generating audit records, or

(c) Overwrite the oldest records, in the case that storage media is unavailable.

Applicability: All	**References:** ARS: AU-5(0); NIST 800-53/53A: AU-5; PISP: 4.3.5	**Related Controls:**

ASSESSMENT PROCEDURE: AU-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for list of actions to be taken by the information system in case of an audit processing failure); information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

AU-6 – Audit Monitoring, Analysis, and Reporting (Low)

Control

Information system audit records shall be reviewed and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and/or suspicious activity. Such activity shall be investigated and reported to appropriate officials, in accordance with current CMS Procedures.

Guidance

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Applicability: All	**References:** ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6	**Related Controls:** AU-4, IR-4

ASSESSMENT PROCEDURE: AU-6.1

Assessment Objective

Determine if:
(i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity;
(ii) the organization investigates suspicious activity or suspected violations;
(iii) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and
(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records.(Optional)
Test: Information system audit monitoring, analysis, and reporting capability.(Optional)

ASSESSMENT PROCEDURE: AU-6.2

Assessment Objective

Determine if the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.(Optional)
Interview: Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities.(Optional)

AU-6(CMS-1) – Enhancement (Low)

Control

Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Applicability: All	**References:** ARS: AU-6(CMS-1); FISCAM: TAC-4.2	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-1).1

Assessment Objective

Determine if:
(i) the organization regularly reviews / analyzes audit records for indications of inappropriate or unusual activity;
(ii) the organization investigates suspicious activity or suspected violations;
(iii) the organization reports findings of inappropriate/usual activities, suspicious behavior, or suspected violations to appropriate officials; and
(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Interview: Organizational personnel responsible for audit and accountability to determine if initialization sequences, log-ons and errors; system processes and performance; and system resource utilization are recorded to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

AU-6(CMS-2) – Enhancement (Low)

Control

Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Applicability: All	**References:** ARS: AU-6(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-2).1

Assessment Objective

Determine if the organization regularly reviews / analyzes audit records for indications of inappropriate or unusual activity.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Interview: Organizational personnel responsible for audit and accountability to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

AU-6(CMS-3) – Enhancement (Low)

Control

Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.

Applicability: All	**References:** ARS: AU-6(CMS-3); FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.3, TAC-4.3.4; HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-3).1

Assessment Objective

Determine if the organization investigates suspicious activity or suspected violations.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.

Interview: Organizational personnel responsible for audit and accountability to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.

AU-6(CMS-4) – Enhancement (Low)

Control

Use automated utilities to review audit records at least once every fourteen (14) days for unusual, unexpected, or suspicious behavior.

Applicability: All	**References:** ARS: AU-6(CMS-4); HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-4).1

Assessment Objective

Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

Interview: Organizational personnel responsible for audit and accountability to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or

suspicious behavior.

AU-6(CMS-5) – Enhancement (Low)

Control

Inspect administrator groups on demand but no less than once every thirty (30) days to ensure unauthorized administrator accounts have not been created.

Applicability: All	**References:** ARS: AU-6(CMS-5); FISCAM: TAC-2.1.5; HIPAA: 164.312(b)	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(CMS-5).1

Assessment Objective

Determine if the organization monitors activities of system administrators.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Interview: Organizational personnel with audit and accountability responsibilities to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

AU-6(FIS-1) – Enhancement (Low)

Control

The use of privileged system software and utilities is reviewed by technical management. Systems programmers' activities are monitored and reviewed. Inappropriate or unusual activity in using utilities is investigated.

Applicability: All	**References:** FISCAM: TSS-2.2.1, TSS-2.2.2, TSS-2.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: AU-6(FIS-1).1

Assessment Objective

Determine if the organization monitors and reviews system programmers' activities and investigates inappropriate or unusual activities when using privileged system software utilities.

Assessment Methods And Objects

Examine: Documentation supporting the supervising and monitoring of systems programmers' activities.
Examine: Documentation supporting their reviews.
Examine: Documentation supporting these investigations.
Examine: Pertinent policies and procedures.
Interview: Systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
Interview: Technical management regarding their reviews of privileged system software and utilities usage.

AU-7 – Audit Reduction and Report Generation (Low)

Control

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to enable human review of audit information and the generation of appropriate audit reports.

Guidance

Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Applicability: All	**References:** ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7	**Related Controls:** AU-4

ASSESSMENT PROCEDURE: AU-7.1

Assessment Objective

Determine if the information system provides an audit reduction and report generation capability.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records.(Optional)
Interview: Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities.(Optional)
Test: Audit reduction and report generation capability.(Optional)

AU-8 – Time Stamps (Low)

Control

Audit records shall employ time stamps for use in audit record generation. Time stamps of audit records shall be generated using internal system clocks that are synchronized system-wide.

Guidance

Time stamps (including date and time) of audit records are generated using internal system clocks.

Applicability: All	**References:** ARS: AU-8; NIST 800-53/53A: AU-8; PISP: 4.3.8	**Related Controls:**

ASSESSMENT PROCEDURE: AU-8.1

Assessment Objective

Determine if the information system provides time stamps for use in audit record generation.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing time stamp generation.(Optional)

AU-9 – Protection of Audit Information (Low)

Control

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

Guidance

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Applicability: All	**References:** ARS: AU-9; NIST 800-53/53A: AU-9; PISP: 4.3.9	**Related Controls:**

ASSESSMENT PROCEDURE: AU-9.1

Assessment Objective

Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records.

Test: Automated mechanisms implementing audit information protection.(Optional)

AU-11 – Audit Record Retention (Low)

Control

Audit records shall be retained to provide support for after-the-fact investigations of security incidents, and to meet regulatory and/or CMS information retention requirements. The National Archives and Records Administration maintains criteria for record retention across many disciplines and information security retention standards shall not be construed to relieve or waive these other standards.

Guidance

The organization retains audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions (CMS sensitive information retention). Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST SP 800-61 provides guidance on computer security incident handling and audit record retention.

Applicability: All	**References:** NIST 800-53/53A: AU-11	**Related Controls:**

ASSESSMENT PROCEDURE: AU-11.1

Assessment Objective

Determine if:

(i) the organization defines the retention period for audit records generated by the information system; and

(ii) the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information system audit record retention responsibilities.(Optional)

AU-11(0) – Enhancement (Low)

Control

Retain audit records for ninety (90) days, and archive old audit records. Retain audit record archives for one (1) year.

Applicability: All	**References:** ARS: AU-11(0); NIST 800-53/53A: AU-11; PISP: 4.3.11	**Related Controls:**

ASSESSMENT PROCEDURE: AU-11(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information system audit record retention responsibilities.(Optional)

Certification, Accreditation, and Security Assessments (CA) – *Management*

CA-1 – Certification, Accreditation, and Security Assessments Policies and Procedures (Low)

Control

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the Business Owner and accredited by the CMS CIO or his/her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the confidentiality, integrity, and availability (CIA) of CMS information and information systems. All C&A and security assessment activities shall be conducted in accordance with current CMS Procedures.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs, MAs, and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and/or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.4.6, Security Accreditation (CA-6).

If the CMS CIO or his/her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his/her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his/her designated representatives.

As part of the system certification and accreditation (C&A), an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, IS Risk Assessment (RA), System Security Plan (SSP), independent system tests and evaluations, the Business Owner and System Developer / Maintainer shall certify that the system meets the security requirements to the extent necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CMS CIO or the Designated Accrediting Authority (DAA).

Guidance

The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CA-1; FISCAM: TSP-5.1.2; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 5.6.1.4#1.1-2; NIST 800-53/53A: CA-1; PISP: 4.4.1	**Related Controls:** CA-6

ASSESSMENT PROCEDURE: CA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security assessment and certification and accreditation policies and procedures;
(ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review policy and procedures; and
(iv) the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.
Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.(Optional)

ASSESSMENT PROCEDURE: CA-1.2

Assessment Objective

Determine if:
(i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.

Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.(Optional)

CA-2 – Security Assessments (Low)

Control

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application, and comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Routine assessments shall be conducted every 365 days, in accordance with NIST SP 800-53 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST SP 800-53 A provides guidance on security control assessments to include reuse of existing assessment results.

Applicability: All	**References:** ARS: CA-2; FISCAM: TSP-5.1.1; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1; NIST 800-53/53A: CA-2; PISP: 4.4.2	**Related Controls:** CA-4, CA-6, CA-7, CA-7(1), SA-11, SI-2

ASSESSMENT PROCEDURE: CA-2.1

Assessment Objective

Determine if:

(i) the information system is in the inventory of major information systems; and

(ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security assessment policy; procedures addressing security assessments; information system security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records.

CA-3 – Information System Connections (Low)

Control

Management shall authorize in writing through the use of system connection agreements all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system connections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

Guidance

Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST SP 800-47 provides guidance on connecting information systems.

Applicability: All	**References:** ARS: CA-3; HSPD 7: F(19); NIST 800-53/53A: CA-3; PISP: 4.4.3	**Related Controls:** SA-9, SC-7

ASSESSMENT PROCEDURE: CA-3.1

Assessment Objective

Determine if:

(i) the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary);

(ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements;
(iii) the organization monitors/controls the system interconnections on an ongoing basis; and
(iv) information system connection agreements are consistent with NIST SP 800-47.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements.(Optional)

CA-3(CMS-1) – Enhancement (Low)

Control

Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

Applicability: All	**References:** ARS: CA-3(CMS-1); FISCAM: TAC-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: CA-3(CMS-1).1

Assessment Objective

Determine if the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.
Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

CA-4 – Security Certification (Low)

Control

Business owners shall conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification process shall be integrated into and span across the SDLC. In addition, the Business Owner shall review the certification documentation every 365 days, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his/her designated representative.

Guidance

A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation.

Applicability: All	**References:** ARS: CA-4; FISCAM: TSS-2.2.4; HSPD 7: F(19); IRS-1075: 6.3#1.1-2; NIST 800-53/53A: CA-4; PISP: 4.4.4	**Related Controls:** CA-2, CA-6, CA-7, SA-11, SI-2

ASSESSMENT PROCEDURE: CA-4.1

Assessment Objective

Determine if:
(i) the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and
(ii) the organization employs a security certification process in accordance with OMB policy and NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with security certification responsibilities.(Optional)

CA-4(CMS-1) – Enhancement (Low)		
Control Document the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures.		
Applicability: All	**References:** ARS: CA-4(CMS-1); HSPD 7: G(24)	**Related Controls:**
ASSESSMENT PROCEDURE: CA-4(CMS-1).1		
Assessment Objective Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities. **Assessment Methods And Objects** **Examine:** Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented. **Interview:** Organizational personnel with security certification responsibilities to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.		
CA-5 – Plan of Action and Milestones (POA&M) (Low)		
Control A POA&M shall be developed, implemented, and updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M shall document the planned, implemented, and evaluated corrective actions to repair deficiencies discovered during the security control assessment, and to reduce or eliminate any known vulnerability in the information system. Personnel shall be designated to assign, track, and update risk mitigation efforts. Designated personnel shall define and authorize corrective action plans, and monitor corrective action progress.		
Guidance The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems. NIST SP 800-30 provides guidance on risk mitigation.		
Applicability: All	**References:** ARS: CA-5; FISCAM: TSP-5.2; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4; NIST 800-53/53A: CA-5; PISP: 4.4.5	**Related Controls:** CA-7
ASSESSMENT PROCEDURE: CA-5.1		
Assessment Objective Determine if: (i) the organization develops and updates at the organization-defined frequency, a plan of action and milestones for the information system; and (ii) the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system. **Assessment Methods And Objects** **Examine:** Certification and accreditation policy; procedures addressing plan of action and milestones; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records. **Interview:** Organizational personnel with plan of action and milestones development and implementation responsibilities.(Optional)		
CA-5(0) – Enhancement (Low)		
Control Develop and submit a plan of action and milestones (POA&M) for any documented information system security finding within thirty (30) days of the final results for every internal / external audit / review or test (e.g., ST&E, penetration test). Update the POA&M monthly until all the findings are resolved.		
Applicability: All	**References:** ARS: CA-5(0); HSPD 7: G(24); NIST 800-53/53A: CA-5; PISP: 4.4.5	**Related Controls:**
ASSESSMENT PROCEDURE: CA-5(0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Certification and accreditation policy and procedures; information system security plan (for organization-defined frequency of plan of action and milestones updates); security assessment		

plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.(Optional)

CA-6 – Security Accreditation (Low)

Control

Explicit authorization to operate the information system shall be received from the CMS CIO or his/her designated representative prior to the system being placed into operations. If the authorization is an interim approval to operate, then the authorization shall be granted based on the designated security category of the information system. An explicit corrective action plan shall be developed, implemented effectively, and monitored by the authorizing official. Re-authorization shall be obtained prior to continued operation:
4.4.6.1. At least every three (3) years;
4.4.6.2. When substantial changes are made to the system;
4.4.6.3. When changes in requirements result in the need to process data of a higher sensitivity;
4.4.6.4. When changes occur to authorizing legislation or federal requirements;
4.4.6.5. After the occurrence of a serious security violation which raises questions about the validity of an earlier certification; and
4.4.6.6. Prior to expiration of a previous accreditation.

Guidance

OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three (3) year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems.

Applicability: All	**References:** ARS: CA-6; FISCAM: TSP-5.1.3, TSP-5.2; HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6	**Related Controls:** CA-1, CA-2, CA-4, CA-7

ASSESSMENT PROCEDURE: CA-6.1

Assessment Objective

Determine if:
(i) the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization in accordance with organization-defined frequency, at least every three (3) years;
(ii) a senior organizational official signs and approves the security accreditation;
(iii) the security accreditation process employed by the organization is consistent with NIST SP 800-37; and
(iv) the organization updates the authorization when there is a significant change to the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST SP 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.
Interview: Organizational personnel with security accreditation responsibilities.(Optional)

CA-6(0) – Enhancement (Low)

Control

Information systems can only be accredited for a maximum period of three (3) years, after which the information system must be re-accredited.

Applicability: All	**References:** ARS: CA-6(0); NIST 800-53/53A: CA-6; PISP: 4.4.6	**Related Controls:**

ASSESSMENT PROCEDURE: CA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST SP 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.

CA-7 – Continuous Monitoring (Low)

Control

Security controls in CMS information systems shall be monitored on an on-going basis. Selection criteria for control monitoring shall be established and a subset of the security controls employed

within information systems shall be selected for continuous monitoring purposes.

Guidance

Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2).

This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST SP 800-37 provides guidance on the continuous monitoring process. NIST SP 800-53 A provides guidance on the assessment of security controls.

Applicability: All	**References:** ARS: CA-7; HSPD 7: F(19); NIST 800-53/53A: CA-7; PISP: 4.4.7	**Related Controls:** CA-2, CA-4, CA-5, CA-6, CM-4, SI-2

ASSESSMENT PROCEDURE: CA-7.1

Assessment Objective

Determine if:
(i) the organization monitors the security controls in the information system on an ongoing basis; and
(ii) the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with continuous monitoring responsibilities.(Optional)

ASSESSMENT PROCEDURE: CA-7.2

Assessment Objective

Determine if:
(i) the organization conducts security impact analyses on changes to the information system;
(ii) the organization documents and reports changes to or deficiencies in the security controls employed in the information system; and
(iii) the organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with continuous monitoring responsibilities.(Optional)

CA-7(1) – Enhancement (Low)

Control

The use of independent certification agents or teams is not required but, if used by the organization to monitor the security controls in the information system on an on-going basis, this can be used to satisfy ST&E requirements.

Guidance

The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle.

Applicability: All	**References:** ARS: CA-7(1); NIST 800-53/53A: CA-7(1)	**Related Controls:** AC-9, CA-2

ASSESSMENT PROCEDURE: CA-7(1).1

Assessment Objective

Determine if the organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.(Optional)

Interview: Organizational personnel with continuous monitoring responsibilities.(Optional)

CA-7(CMS-1) – Enhancement (Low)

Control

Continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and
(e) Status reporting.

Applicability: All	**References:** ARS: CA-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: CA-7(CMS-1).1

Assessment Objective

Determine if:
(i) the organization monitors the security controls in the information system on an ongoing basis; and
(ii) the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records to determine continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and
(e) Status reporting.

Interview: Organizational personnel with continuous monitoring responsibilities to determine continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and
(e) Status reporting.

Configuration Management (CM) – *Operational*

CM-1 – Configuration Management Policy and Procedures (Low)

Control

A CM process that includes the approval, testing, implementation, and documentation of changes shall be developed, documented, and implemented effectively to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with the organization's information technology architecture plans. Formally documented CM roles, responsibilities, procedures, and documentation shall be in place.

Guidance

The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CM-1; FISCAM: TCC-2.1.9, TCC-3.2.1, TCC-3.2.2, TCC-3.3.1, TSS-3.1.1, TSS-3.1.2, TSS-3.1.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-1; PISP: 4.5.1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents configuration management policy and procedures;
(ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review configuration management policy and procedures; and
(iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.
Interview: Organizational personnel with configuration management and control responsibilities.(Optional)

ASSESSMENT PROCEDURE: CM-1.2

Assessment Objective

Determine if:
(i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.
Interview: Organizational personnel with configuration management and control responsibilities.(Optional)

CM-2 – Baseline Configuration (Low)

Control

A baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system shall be developed and documented. Procedures shall be developed, documented, and implemented effectively to maintain the baseline configuration. The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture.

Guidance

This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture.

Applicability: All	**References:** ARS: CM-2; HIPAA: 164.310(b); NIST 800-53/53A: CM-2; PISP: 4.5.2	**Related Controls:** CM-6, CM-8

ASSESSMENT PROCEDURE: CM-2.1

Assessment Objective

Determine if:
(i) the organization develops, documents, and maintains a baseline configuration of the information system;

(ii) the baseline configuration shows relationships among information system components and is consistent with the Federal Enterprise Architecture;
(iii) the baseline configuration provides the organization with a well-defined and documented specification to which the information system is built; and
(iv) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.

CM-2(CMS-1) – Enhancement (Low)

Control

Review and, if necessary, update the baseline configuration and any other system-related operations or security documentation at least once every year, and while planning major system changes / upgrades.

Applicability: All	**References:** ARS: CM-2(CMS-1); FISCAM: TSS-3.2.6	**Related Controls:**

ASSESSMENT PROCEDURE: CM-2(CMS-1).1

Assessment Objective

Determine if the organization develops, documents, and maintains a baseline configuration of the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records to determine the baseline configuration and any other system-related operations or security documentation are reviewed and updated at least once every year, and while planning major system changes / upgrades.

Interview: Organizational personnel with configuration management responsibilities to determine the baseline configuration and any other system-related operations or security documentation are reviewed and updated at least once every year, and while planning major system changes / upgrades.

CM-2(CMS-2) – Enhancement (Low)

Control

Maintain an updated list of the information system's operations and security documentation.

Applicability: All	**References:** ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6	**Related Controls:**

ASSESSMENT PROCEDURE: CM-2(CMS-2).1

Assessment Objective

Determine if the organization updates the baseline configuration of the information system as an integral part of information system component installations.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records to determine an updated list of the information system's operations and security documentation is maintained.

Interview: Organizational personnel with configuration management responsibilities to determine an updated list of the information system's operations and security documentation is maintained.

CM-3 – Configuration Change Control (Low)

Control

Change control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to control changes to the information system. Change request forms shall be used to document requests with related approvals. Change requests shall be approved by the Business Owner, or his/her designated representative, and other appropriate organization officials including, but not limited to, the system maintainer and information system support staff.

Test plans shall be developed and approved for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control) and shall include appropriate consideration of security. Test results shall be documented and appropriate responsive actions shall be taken based on the results.

Emergency changes for the CMS information system shall be documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration shall be documented appropriately and approved, and responsible personnel shall be notified for security analysis and follow-up.

Guidance

The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the

security analysis of the change. The organization audits activities associated with configuration changes to the information system.

Applicability: All	**References:** ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3	**Related Controls:** CM-4, CM-6, SI-2

ASSESSMENT PROCEDURE: CM-3.1

Assessment Objective

Determine if:
(i) the organization authorizes, documents, and controls changes to the information system;
(ii) the organization manages configuration changes to the information system using an organizationally approved process;
(iii) the organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws; and
(iv) the organization audits activities associated with configuration changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system configuration change control; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.(Optional)

CM-3(FIS-1) – Enhancement (Low)

Control

Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.

Applicability: All	**References:** FISCAM: TCC-2.1.11	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-1).1

Assessment Objective

Determine if the organization reviews production program changes for access and change control compliance.

Assessment Methods And Objects

Examine: Documentation of management or security administrator reviews.
Examine: Pertinent policies and procedures.
Interview: Information system management or security administrators.

CM-3(FIS-2) – Enhancement (Low)

Control

Migration of tested and approved system software to production use is performed by an independent library control group.

Applicability: All	**References:** FISCAM: TSS-3.2.2	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-2).1

Assessment Objective

Determine if the organizational independent library control group migrates tested and approved software into production.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Supporting documentation for some system software migrations.
Interview: Management, systems programmers, and library control personnel, and determine who migrates approved system software to production libraries.

CM-3(FIS-3) – Enhancement (Low)

Control

Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.

Applicability: All	**References:** FISCAM: TSS-3.2.1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-3).1

Assessment Objective

Determine if the organization provides advance schedules to system users which minimize system software installation impacts.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Examine: Recent installations and determine whether scheduling and advance notification did occur.

Interview: Management and systems programmers about scheduling and giving advance notices when system software is installed.

CM-3(FIS-4) – Enhancement (Low)

Control

Outdated versions of system software are removed from production libraries.

Applicability: All	**References:** FISCAM: TSS-3.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: CM-3(FIS-4).1

Assessment Objective

Determine if the organization removes outdated versions of system software from the production libraries.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation for the removal of outdated versions from production libraries.

Interview: Management, systems programmers, and library control personnel, and determine whether outdated versions are removed from production libraries.

CM-5 – Access Restrictions for Change (Low)

Control

Access control change mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to approve individual access privileges and to enforce physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.

Guidance

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

Applicability: All	**References:** ARS: CM-5; FISCAM: TCC-3.2.3, TCC-3.3.1, TSS-1.2.1, TSS-1.2.2, TSS-3.1.4, TSS-3.2.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-5; PISP: 4.5.5	**Related Controls:**

ASSESSMENT PROCEDURE: CM-5.1

Assessment Objective

Determine if:

(i) the organization maintains a list of qualified and authorized personnel permitted to access the information system for the express purpose of initiating changes;

(ii) the organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and

(iii) the organization generates, retains, and reviews records reflecting all such changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.(Optional)

Test: Change control process and associated restrictions for changes to the information system.(Optional)

CM-6 – Configuration Settings (Low)

Control

Procedures shall be developed, documented, and implemented effectively to configure and benchmark information technology products in accordance with good security practice settings. Mandatory configuration settings for information technology products employed within the information system shall be established. The security settings of information technology products shall be configured to the most restrictive mode consistent with information system operational requirements, documented, and enforced in all components of the information system.

Guidance

Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems.

Applicability: All	**References:** ARS: CM-6; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6; PISP: 4.5.6	**Related Controls:** CM-2, CM-3, CM-8, SI-4

ASSESSMENT PROCEDURE: CM-6.1

Assessment Objective

Determine if:

(i) the organization establishes mandatory configuration settings for information technology products employed within the information system;

(ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;

(iii) the organization documents the configuration settings; and
(iv) the organization enforces the configuration settings in all components of the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST SP 800-70; other relevant documents or records.
Test: Information system configuration settings.(Optional)

CM-6(CMS-1) – Enhancement (Low)

Control

Configure the information system to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

Applicability: All	**References:** ARS: CM-6(CMS-1); IRS-1075: 5.6.2.3#1	**Related Controls:**

ASSESSMENT PROCEDURE: CM-6(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes mandatory configuration settings for information technology products employed within the information system;
(ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; and
(iii) the organization documents the configuration settings.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST SP 800-70; other relevant documents or records to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.
Interview: Organizational personnel with configuration management responsibilities to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

CM-8 – Information System Component Inventory (Low)

Control

Procedures shall be developed, documented, and implemented effectively to document and maintain a current inventory of the information system's constituent components and relevant ownership information. The inventory of information system components shall include manufacturer, model / type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership.

Guidance

The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system.

Applicability: All	**References:** ARS: CM-8; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8; PISP: 4.5.8	**Related Controls:** CM-2, CM-6

ASSESSMENT PROCEDURE: CM-8.1

Assessment Objective

Determine if:
(i) the organization develops, documents, and maintains a current inventory of the components of the information system; and
(ii) the inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system inventory records; other relevant documents or records.

Contingency Planning (CP) – *Operational*

CP-1 – Contingency Planning Policy and Procedures (Low)

Control

All major CMS information systems shall be covered by a CP that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

Guidance

The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-34 provides guidance on contingency planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: CP-1; FISCAM: TSC-2.2.2; HIPAA: 164.308(a)(7)(i), 164.308(a)(7)(ii)(B); IRS-1075: 5.6.2.2#1.1; NIST 800-53/53A: CP-1; PISP: 4.6.1	**Related Controls:**

ASSESSMENT PROCEDURE: CP-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents contingency planning policy and procedures;
(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and
(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: CP-1.2

Assessment Objective

Determine if:
(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

CP-2 – Contingency Plan (Low)

Control

All major CMS information systems shall be covered by a CP, relative to the system security level, providing continuity of support in the event of a disruption of service. A CP for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A CP for the information system shall be consistent with NIST SP 800-34. Designated officials within the organization shall review and approve the CP and distribute copies of the plan to key contingency personnel.

Guidance

Contingency Plans consist of all components listed in the CMS Business Partners system Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.

Applicability: All	**References:** ARS: CP-2; FISCAM: TSC-1.1, TSC-1.2, TSC-1.3, TSC-2.1.2, TSC-3.1.1, TSC-3.1.2, TSC-3.1.3, TSC-3.1.4, TSC-3.2.3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.3; NIST 800-53/53A: CP-2; PISP: 4.6.2	**Related Controls:**

ASSESSMENT PROCEDURE: CP-2.1

Assessment Objective

Determine if:

(i) the organization develops and documents a contingency plan for the information system;
(ii) the contingency plan is consistent with NIST SP 800-34;
(iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure;
(iv) the contingency plan is reviewed and approved by designated organizational officials; and
(v) the organization disseminates the contingency plan to key contingency personnel.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; NIST SP 800-34; contingency plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-2.2

Assessment Objective

Determine if key contingency personnel and the key operating elements within the organization understand the contingency plan and are ready to implement the plan.

Assessment Methods And Objects

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

CP-3 – Contingency Training (Low)

Control

Operational and support personnel (including managers and users of the information system) shall receive training in contingency operations and understand their contingency roles and responsibilities with respect to the information system. Refresher training shall be provided to all contingency personnel.

Guidance

Managers, responsible for contingency operations, and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirmed that appropriate training has been completed.

Applicability: All	**References:** ARS: CP-3; FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3	**Related Controls:**

ASSESSMENT PROCEDURE: CP-3.1

Assessment Objective

Determine if:
(i) the organization provides contingency training to personnel with significant contingency roles and responsibilities;
(ii) the organization records the type of contingency training received and the date completed;
(iii) the organization defines frequency of refresher contingency training; and
(iv) the organization provides initial training and refresher training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan; other relevant documents or records.(Optional)
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.(Optional)

ASSESSMENT PROCEDURE: CP-3.2

Assessment Objective

Determine if contingency training material addresses the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.(Optional)

CP-3(0) – Enhancement (Low)

Control

Provide training every 365 days in contingency roles and responsibilities.

Applicability: All	**References:** ARS: CP-3(0); FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); PISP: 4.6.3	**Related Controls:**

ASSESSMENT PROCEDURE: CP-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan

(for organization-defined frequency for refresher contingency training); other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-4 – Contingency Plan Testing and Exercises (Low)

Control

CPs shall be tested and/or exercised at least every 365 days using defined tests and exercises, such as the tabletop test in accordance with current CMS Procedures, to determine the plans' effectiveness and readiness to execute the plan. Test / exercise results shall be documented and reviewed by appropriate organization officials. Reasonable and appropriate corrective actions shall be initiated to close or reduce the impact of CP failures and deficiencies.

Guidance

There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Applicability: All	References: ARS: CP-4; FISCAM: TSC-1.1, TSC-4.1, TSC-4.2.1, TSC-4.2.2; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2; NIST 800-53/53A: CP-4; PISP: 4.6.4	Related Controls:

ASSESSMENT PROCEDURE: CP-4.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of contingency plan tests and/or exercises;
(ii) the organization defines the set of contingency plan tests and/or exercises;
(iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;
(iv) the organization documents the results of contingency plan testing/exercises; and
(v) the organization reviews the contingency plan test/exercise results and takes corrective actions.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-4.2

Assessment Objective

Determine if the contingency plan tests/exercises address key aspects of the plan.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records.

CP-4(0) – Enhancement (Low)

Control

The CP must be current and executable, tested using a combination of tabletop exercises and operational tests every 365 days, and updated as needed.

Applicability: All	References: ARS: CP-4(0); FISCAM: TSC-4.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-4; PISP: 4.6.4	Related Controls:

ASSESSMENT PROCEDURE: CP-4(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan (for the organization-defined frequency of contingency plan tests and/or exercises and the list of the organization-defined contingency plan tests and/or exercises); contingency plan testing and/or exercise documentation; other relevant documents or records.

CP-5 – Contingency Plan Update (Low)

Control

CPs shall be reviewed at least every 365 days and, if necessary, revised to address system / organizational changes and/or any problems encountered during plan implementation, execution, or

testing.

Guidance

Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Applicability: All	**References:** ARS: CP-5; FISCAM: TSC-1.1, TSC-3.1.5; HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	**Related Controls:**

ASSESSMENT PROCEDURE: CP-5.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of contingency plan reviews and updates;
(ii) the organization updates the contingency plan in accordance with organization-defined frequency, at least annually; and
(iii) the revised plan addresses the system/organizational changes identified by the organization or any problems encountered by the organization during plan implementation, execution, and testing.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-5.2

Assessment Objective

Determine if the organization communicates necessary changes to the contingency plan to other organizational elements with related plans.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records.(Optional)
Interview: Organizational personnel with contingency plan update responsibilities; organizational personnel with mission-related and operational responsibilities.(Optional)

CP-5(0) – Enhancement (Low)

Control

Review the CP at least every 365 days and update, as necessary, to address: system, organizational, or facility changes; problems encountered during plan implementation, execution, or testing; or other conditions that may impact the system CP.

Applicability: All	**References:** ARS: CP-5(0); HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	**Related Controls:**

ASSESSMENT PROCEDURE: CP-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan (for organization-defined frequency of contingency plan reviews and updates); other relevant documents or records.
Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records.(Optional)
Interview: Organizational personnel with contingency plan review and update responsibilities; organizational personnel with mission-related and operational responsibilities.(Optional)

CP-9 – Information System Backup (Low)

Control

Backup mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable the backing-up of user-level and system-level information (including system state information) contained in the CMS information system. The frequency of information system backups and the transfer rate of backup information to an alternate storage site (if so designated) shall be consistent with the CMS recovery time objectives and recovery point objectives.

Mechanisms shall provide for sufficient backup storage capability. Checkpoint capabilities shall be part of any backup operation that updates files and consumes large amounts of information system time. Backup copies of CMS data shall be created on a regular basis, and appropriate safeguards shall be implemented to protect the technical and physical security of backup media at the storage location. Where appropriate, backup copies of all other forms of data, including paper records, shall be created based upon an assessment of the level of data criticality and the corresponding risk of data loss.

Guidance

The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup

information. Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time. The protection of system backup information while in transit is beyond the scope of this control.

Applicability: All	**References:** ARS: CP-9; FISCAM: TSC-2.1.1, TSC-2.1.3; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	**Related Controls:** MA-CMS-1, MA-CMS-2, MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of information systems backups;
(ii) the organization defines the user-level and system-level information (including system state information) that is required to be backed up; and
(iii) the organization identifies the location(s) for storing backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records.

ASSESSMENT PROCEDURE: CP-9.2

Assessment Objective

Determine if:
(i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency;
(ii) the organization stores backup information in designated locations in accordance with information system backup procedures; and
(iii) the organization protects backup information at the designated storage locations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records.

CP-9(0) – Enhancement (Low)

Control

Perform backups of user-level and system-level information (including system state information) every month.

Applicability: All	**References:** ARS: CP-9(0); HIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	**Related Controls:**

ASSESSMENT PROCEDURE: CP-9(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for information system backup); backup storage location(s); other relevant documents or records.

CP-10 – Information System Recovery and Reconstitution (Low)

Control

Information system recovery and reconstitution mechanisms with supporting procedures shall be developed, documented, and implemented effectively to allow the CMS information system to be recovered and reconstituted to a known secure state after a disruption or failure. Recovery of CMS information systems after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

Guidance

Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Applicability: All	**References:** ARS: CP-10; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10; PISP: 4.6.10	**Related Controls:**

ASSESSMENT PROCEDURE: CP-10.1

Assessment Objective

Determine if the organization identifies the means for capturing the information system's operational state including appropriate system parameters, patches, configuration settings, and

application/system software prior to system disruption or failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-10.2

Assessment Objective

Determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

Test: Automated mechanisms implementing information system recovery and reconstitution operations.(Optional)

CP-10(0) – Enhancement (Low)

Control

Secure information system recovery and reconstitution includes, but not limited to:
(a) Reset all system parameters (either default or organization-established),
(b) Reinstall patches,
(c) Reestablish configuration settings,
(d) Reinstall application and system software, and
(e) Fully test the system.

Applicability: All	**References:** ARS: CP-10(0); NIST 800-53/53A: CP-10; PISP: 4.6.10	**Related Controls:**

ASSESSMENT PROCEDURE: CP-10(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Identification and Authentication (IA) – *Technical*

IA-1 – Identification and Authentication Policy and Procedures (Low)

Control

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

Guidance

The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and SP 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**References:** ARS: IA-1; IRS-1075: 5.6.3.1#1.1; NIST 800-53/53A: IA-1; PISP: 4.7.1	**Related Controls:**

ASSESSMENT PROCEDURE: IA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents identification and authentication policy and procedures;
(ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review identification and authentication policy and procedures; and
(iv) the organization updates identification and authentication policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.
Interview: Organizational personnel with identification and authentication responsibilities.(Optional)

ASSESSMENT PROCEDURE: IA-1.2

Assessment Objective

Determine if:
(i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.
Interview: Organizational personnel with identification and authentication responsibilities.(Optional)

IA-2 – User Identification and Authentication (Low)

Control

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique IA of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

Guidance

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in SP 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST SP 800-63 level 1 compliant. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST SP 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals.

Applicability: All	**References:** ARS: IA-2; FISCAM: TAC-3.2.A.4, TAN-2.1.4; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 5.6.3.1#1.2, 5.6.3.3#2.3; NIST 800-53/53A: IA-2; PISP: 4.7.2	**Related Controls:** AC-14, AC-17, MA-4

ASSESSMENT PROCEDURE: IA-2.1

Assessment Objective

Determine if:
(i) the information system uniquely identifies and authenticates users (or processes acting on behalf of users); and
(ii) authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63 and e-authentication risk assessment results.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; e-authentication risk assessment results; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Test: Automated mechanisms implementing identification and authentication capability for the information system.(Optional)

IA-2(CMS-1) – Enhancement (Low)

Control

Require the use of unique user identifiers and system and/or network authenticators.

Applicability: All	**References:** ARS: IA-2(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4, TAN-2.1.4, TAN-2.1.7; IRS-1075: 5.6.3.1#1.2	**Related Controls:**

ASSESSMENT PROCEDURE: IA-2(CMS-1).1

Assessment Objective

Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine the use of unique user identifiers and system and/or network authenticators is required.
Interview: Organizational personnel with identification and authentication responsibilities to determine the use of unique user identifiers and system and/or network authenticators is required.

IA-2(CMS-2) – Enhancement (Low)

Control

All passwords shall be encrypted in transit and at rest.

Applicability: All	**References:** ARS: IA-2(CMS-2); FISCAM: TAC-3.2.A.1, TAC-3.2.A.7; IRS-1075: 5.6.3.1#1.2	**Related Controls:**

ASSESSMENT PROCEDURE: IA-2(CMS-2).1

Assessment Objective

Determine if authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine all passwords are required to be encrypted in transit and at rest.
Interview: Organizational personnel with identification and authentication responsibilities to determine to determine all passwords are required to be encrypted in transit and at rest.

IA-2(CMS-3) – Enhancement (Low)

Control

Help desk support requires user identification for any transaction that has information security implications.

Applicability: All	**References:** ARS: IA-2(CMS-3)	**Related Controls:**

ASSESSMENT PROCEDURE: IA-2(CMS-3).1

Assessment Objective

Determine if authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine help desk support requires user identification for any transaction that has information security implications.

Interview: Organizational personnel with identification and authentication responsibilities to determine to determine help desk support requires user identification for any transaction that has information security implications.

IA-3 – Device Identification and Authentication (Low)

Control

Automated mechanisms shall be used to enable IA of the CMS information system being used and to which a connection is being made before establishing a connection.

Guidance

The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802. 1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Applicability: All	**References:** ARS: IA-3; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	**Related Controls:**

ASSESSMENT PROCEDURE: IA-3.1

Assessment Objective

Determine if:
(i) the organization defines specific devices requiring identification and authentication before establishing connections to the information system; and
(ii) the information system identifies and authenticates specific devices identified by the organization before establishing connections.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing device identification and authentication.(Optional)

IA-3(0) – Enhancement (Low)

Control

Implement an information system that uses either a shared secret or digital certificate to identify and authenticate specific devices before establishing a connection.

Applicability: All	**References:** ARS: IA-3(0); IRS-1075: 5.6.3.1#1.2; PISP: 4.7.3	**Related Controls:**

ASSESSMENT PROCEDURE: IA-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; information system design documentation; procedures addressing device identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.

IA-4 – Identifier Management (Low)

Control

Procedures shall be developed, documented, and implemented effectively to manage user identifiers. The procedures shall address processes and controls for:
4.7.4.1. Identifying each user uniquely;
4.7.4.2. Verifying the identity of each user;
4.7.4.3. Receiving authorization to issue a user identifier from an appropriate organization official;
4.7.4.4. Ensuring that the user identifier is issued to the intended party;
4.7.4.5. Disabling user identifier after a specific period of inactivity; and
4.7.4.6. Archiving user identifiers.

Reviews and validation of system users' accounts shall be conducted to ensure the continued need for access to a system. Identifier management shall not be applicable to shared information system accounts (i.e., guest and anonymous).

Guidance

Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity

verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors.

Applicability: All	**References:** ARS: IA-4; FISCAM: TAC-3.2.A.4, TAN-2.1.4; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-4; PISP: 4.7.4	**Related Controls:**

ASSESSMENT PROCEDURE: IA-4.1

Assessment Objective

Determine if:
(i) the organization manages user identifiers by uniquely identifying each user;
(ii) the organization manages user identifiers by verifying the identity of each user;
(iii) the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official;
(iv) the organization manages user identifiers by issuing the identifier to the intended party;
(v) the organization defines the time period of inactivity after which a user identifier is to be disabled;
(vi) the organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and
(vii) the organization manages user identifiers by archiving identifiers.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Identity verification capability for the information system and for organizational facilities.(Optional)

ASSESSMENT PROCEDURE: IA-4.2

Assessment Objective

Determine if the organization uses a Personal Identity Verification (PIV) card token to uniquely identify and authenticate federal employees and contractors in accordance with FIPS 201 and NIST SP 800-73, 800-76, and 800-78.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST SP 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Identity verification capability for the information system and for organizational facilities.(Optional)

IA-4(0) – Enhancement (Low)

Control

Disable user identifiers after 365 days of inactivity and delete disabled accounts during annual re-certification process.

Applicability: All	**References:** ARS: IA-4(0); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.1#2, 5.6.3.2#2.1; NIST 800-53/53A: IA-4; PISP: 4.7.4	**Related Controls:** AC-2(3)

ASSESSMENT PROCEDURE: IA-4(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST SP 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

IA-4(CMS-1) – Enhancement (Low)

Control

Require system administrator to maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.

Applicability: All	**References:** ARS: IA-4(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4; IRS-1075: 5.6.3.1#2	**Related Controls:** AC-2(CMS-2)

ASSESSMENT PROCEDURE: IA-4(CMS-1).1

Assessment Objective

Determine if the organization manages user identifiers by uniquely identifying each user.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.

Interview: Organizational personnel with identification and authentication responsibilities to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.

IA-4(CMS-2) – Enhancement (Low)

Control

For non-CMS entities to issue user identifiers, receive prior written approval from the CIO or his/her designated representative.

Applicability: All	**References:** ARS: IA-4(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: IA-4(CMS-2).1

Assessment Objective

Determine if responsible parties within the organization periodically review identification and authentication policy and procedures.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers.

Interview: Organizational personnel with identification and authentication management responsibilities to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers.

IA-4(FIS-1) – Enhancement (Low)

Control

Personnel files are matched with actual system users to remove terminated or transferred employees from the system.

Applicability: All	**References:** FISCAM: TAC-3.2.A.6	**Related Controls:**

ASSESSMENT PROCEDURE: IA-4(FIS-1).1

Assessment Objective

Determine if the organizational personnel files are matched with actual system users to remove terminated or transferred employees from the system.

Assessment Methods And Objects

Examine: Documentation of such comparisons.

Examine: Pertinent policies and procedures.

Interview: Security managers.

IA-5 – Authenticator Management (Low)

Control

Procedures shall be developed, documented, and implemented effectively to manage user authenticators. The procedures shall address processes and controls for: initial authenticator content; distribution for new, lost, compromised, or damaged authenticators; revocation of authenticators; changing default authenticators; and changing / refreshing authenticators at specified intervals. Users shall not loan or share authenticators with other users. Lost or compromised authenticators shall be reported immediately to appropriate authority.

Selection of passwords or other authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS System Security Level of the information system. Automated mechanisms shall be in place for password-based authentication, to ensure that the information system:

4.7.5.1. Protects passwords from unauthorized disclosure and modification when stored and transmitted;

4.7.5.2. Prohibits passwords from being displayed when entered;

4.7.5.3. Enforces automatic expiration of passwords;

4.7.5.4. Prohibits password reuse for a specified number of generations; and

4.7.5.5. Enforces periodic password changes.

Guidance

Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i)

validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**References:** ARS: IA-5; FISCAM: TAC-3.2.A.1, TAC-3.2.A.3; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	**Related Controls:** AC-11(0), AC-CMS-1(CMS-2)

ASSESSMENT PROCEDURE: IA-5.1

Assessment Objective

Determine if:
(i) the organization manages information system authenticators by defining initial authenticator content;
(ii) the organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;
(iii) the organization manages information system authenticators by changing default authenticators upon information system installation; and
(iv) the organization manages information system authenticators by changing/refreshing authenticators periodically.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.
Test: Automated mechanisms implementing authenticator management functions.(Optional)

IA-5(0) – Enhancement (Low)

Control

For password-based authentication:
(a) Protect passwords from disclosure or modification when stored or transmitted,
(b) Prevent passwords from being displayed when entered,
(c) When using passwords in connection with e-authentication, refer to ARS Appendix A, e-Authentication Standards for further guidance,
(d) Force users to select a password comprising a minimum of eight (8) alphanumeric and/or special characters,
(e) Automatically force users (including administrators) to change account and system account passwords every sixty (60) days,
(f) Automatically force users to select one (1) unique passwords prior to reusing a previous one, and
(g) Enforce password lifetime restrictions within a minimum of one (1) day and maximum of sixty (60) days.

Applicability: All	**References:** ARS: IA-5(0); HIPAA: 164.308(a)(5)(ii)(D); IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

IA-5(FIS-1) – Enhancement (Low)

Control

For devices such as tokens or key cards, users: (1) maintain possession of their individual tokens, cards, etc., and (2) understand that they must not loan or share these with others, and must report lost items immediately.

Applicability: All	**References:** FISCAM: TAC-3.2.A.8	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(FIS-1).1

Assessment Objective

Determine if:
(i) the organizational users maintain possession of their individual devices such as tokens or key cards, etc.; and
(ii) the organizational users understand they must not loan or share their individual tokens, cards, etc., and report lost items immediately.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Token or key card acknowledgment forms.
Interview: Token and/or key card users.

IA-5(DIR-1) – Enhancement (Low)

Control

For password-based authentication, passwords are:
(a) unique for specific individuals, not groups;
(b) controlled by the assigned user and not subject to disclosure;
(c) not displayed when entered;
(d) changed every 60 days, when an individual changes positions, or when security is breached;
(e) at least 8 characters in length;
(f) must include at least one number, one upper and lower case character, and one special character;
(g) prohibited from reuse for at least 6 generations;
(h) prohibited from being changed more than once in a 24-hour period; and
(i) all passwords are encrypted in transit and at rest. The use of dictionary names or words as passwords is prohibited.

Applicability: All	**References:** FISCAM: TAC-3.2.A.1, TAC-3.2.A.2, TAN-2.1.4	**Related Controls:**

ASSESSMENT PROCEDURE: IA-5(DIR-1).1

Assessment Objective

Determine if the organization effectively uses password and user identification as one tool for security in-depth.

Assessment Methods And Objects

Examine: Password and user identification policy and acceptable user training policy for completeness in meeting the CMS password controls.
Interview: A sampling of users know the organization's policy for password and user system identification.

IA-6 – Authenticator Feedback (Low)

Control

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to obscure feedback to users during the authentication process to protect the information from possible exploitation / use by unauthorized individuals.

Guidance

The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Applicability: All	**References:** ARS: IA-6; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-6; PISP: 4.7.6	**Related Controls:**

ASSESSMENT PROCEDURE: IA-6.1

Assessment Objective

Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing authenticator feedback.(Optional)

IA-6(0) – Enhancement (Low)

Control

Configure the information system to obscure passwords during the authentication process (e.g., display asterisks).

Applicability: All	**References:** ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6	**Related Controls:**

ASSESSMENT PROCEDURE: IA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-7 – Cryptographic Module Authentication (Low)		
Control Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.		
Guidance The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.		
Applicability: All	**References:** ARS: IA-7; NIST 800-53/53A: IA-7; PISP: 4.7.7	**Related Controls:**
ASSESSMENT PROCEDURE: IA-7.1		
Assessment Objective Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended). **Assessment Methods And Objects** **Examine:** Identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test:** Automated mechanisms implementing cryptographic module authentication.(Optional)		

Incident Response (IR) – *Operational*

IR-1 – Incident Response Policy and Procedures (Low)

Control

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed, documented, and implemented effectively to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-61 and current CMS Procedures.

Guidance

The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

Applicability: All	**References:** ARS: IR-1; FISCAM: TSP-3.4; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1; NIST 800-53/53A: IR-1; PISP: 4.8.1	**Related Controls:**

ASSESSMENT PROCEDURE: IR-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents incident response policy and procedures;
(ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review incident response policy and procedures; and
(iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.
Interview: Organizational personnel with incident response planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: IR-1.2

Assessment Objective

Determine if:
(i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.
Interview: Organizational personnel with incident response planning and plan implementation responsibilities.(Optional)

IR-4 – Incident Handling (Low)

Control

An incident handling capability, which includes preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents, shall be established and maintained. Evidence of computer crimes, computer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learned from on-going incident handling activities shall be incorporated into the IR procedures.

Guidance

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.

Applicability: All	**References:** ARS: IR-4; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4; PISP: 4.8.4	**Related Controls:** AU-6, PE-6, SI-2

ASSESSMENT PROCEDURE: IR-4.1

Assessment Objective

Determine if:
(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and

(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling; NIST SP 800-61; other relevant documents or records.

Interview: Organizational personnel with incident handling responsibilities.(Optional)

Test: Incident handling capability for the organization.(Optional)

IR-4(CMS-1) – Enhancement (Low)

Control

Document relevant information related to a security incident according to CMS Information Security Incident Handling and Breach Notification Procedures.

Applicability: All	**References:** ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-4(CMS-1).1

Assessment Objective

Determine if:

(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and

(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if relevant information related to a security incident is documented according to the CMS Information Security Incident Handling and Breach Notification Procedures.

Interview: Organizational personnel with incident response training and operational responsibilities to determine if relevant information related to a security incident is documented according to the CMS Information Security Incident Handling and Breach Notification Procedures.

IR-4(CMS-2) – Enhancement (Low)

Control

Preserve evidence through technical means, including secured storage of evidence media and “write” protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.

Applicability: All	**References:** ARS: IR-4(CMS-2); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-4(CMS-2).1

Assessment Objective

Determine if:

(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and

(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if evidence is preserved through technical means, including secured storage of evidence media and “write” protection of evidence media; sound forensics processes and utilities are used that support legal requirements. A chain of custody for forensic evidence is followed.

Interview: Organizational personnel with incident response training and operational responsibilities to determine if evidence is preserved through technical means, including secured storage of evidence media and “write” protection of evidence media; sound forensics processes and utilities are used that support legal requirements. A chain of custody for forensic evidence is followed.

IR-4(CMS-3) – Enhancement (Low)

Control

Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure.

Applicability: All	**References:** ARS: IR-4(CMS-3); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls:**

ASSESSMENT PROCEDURE: IR-4(CMS-3).1

Assessment Objective

Determine if:

(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and

(ii) the incident handling capability is consistent with NIST SP 800-61.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents or records to determine if the identification of vulnerabilities exploited during a security incident and security safeguards are implemented to reduce risk and vulnerability exploit exposure.

Interview: Organizational personnel with incident response training and operational responsibilities to determine if the identification of vulnerabilities exploited during a security incident and security safeguards are implemented to reduce risk and vulnerability exploit exposure.

IR-6 – Incident Reporting (Low)

Control

All IS incidents, or suspected incidents, shall be reported to the CMS IT Service Desk (or equivalent organizational function) as soon as an incident comes to the attention of a user of CMS information or information systems. Events and confirmed security incidents by business partners shall also be reported to the CMS IT Service Desk in accordance with established procedures.

Guidance

The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST SP 800-61 provides guidance on incident reporting.

Applicability: All	**References:** ARS: IR-6; FISCAM: TAC-4.2; NIST 800-53/53A: IR-6; PISP: 4.8.6	**Related Controls:**

ASSESSMENT PROCEDURE: IR-6.1

Assessment Objective

Determine if:
(i) the organization promptly reports incident information to appropriate authorities;
(ii) incident reporting is consistent with NIST SP 800-61;
(iii) the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and
(iv) weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident reporting; NIST SP 800-61; incident reporting records and documentation; other relevant documents or records.
Interview: Organizational personnel with incident reporting responsibilities.(Optional)
Test: Incident reporting capability for the organization.(Optional)

IR-7 – Incident Response Assistance (Low)

Control

A CMS IT Service Desk (or equivalent organizational function) shall be in place and shall play an appropriate role in the organization's IR program. The CMS IT Service Desk shall offer advice to users of a CMS information system. Procedures shall be developed, documented, and implemented effectively to facilitate the incident response by providing central incident support resource for CMS information system users.

Guidance

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

Applicability: All	**References:** ARS: IR-7; NIST 800-53/53A: IR-7; PISP: 4.8.7	**Related Controls:**

ASSESSMENT PROCEDURE: IR-7.1

Assessment Objective

Determine if:
(i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and
(ii) the incident response support resource is an integral part of the organization's incident response capability.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; other relevant documents or records.
Interview: Organizational personnel with incident response assistance and support responsibilities.(Optional)

Maintenance (MA) – *Operational*

MA-1 – System Maintenance Policy and Procedures (Low)

Control

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

Guidance

The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: MA-1; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-1; PISP: 4.9.1	**Related Controls:**

ASSESSMENT PROCEDURE: MA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents information system maintenance policy and procedures;
(ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review information system maintenance policy and procedures; and
(iv) the organization updates information system maintenance policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

ASSESSMENT PROCEDURE: MA-1.2

Assessment Objective

Determine if:
(i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-1(FIS-1) – Enhancement (Low)

Control

All system software is current, has current and complete documentation, and is still supported by the vendor.

Applicability: All	**References:** FISCAM: TSS-3.2.5, TSS-3.2.6	**Related Controls:**

ASSESSMENT PROCEDURE: MA-1(FIS-1).1

Assessment Objective

Determine if the organization uses current system software with complete documentation and is vendor supported.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.
Interview: Management and systems programmers about the currency of system software, and the currency and completeness of software documentation.
Interview: System software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.

MA-2 – Controlled Maintenance (Low)

Control

Comprehensive maintenance procedures shall be developed, documented, and implemented effectively to conduct controlled periodic on-site and off-site maintenance of the CMS information

systems and of the physical plant within which these information systems reside. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS-approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly.

Guidance

All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Applicability: All; Optional for SS	**References:** ARS: MA-2; FISCAM: TSC-2.4.1, TSC-2.4.2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-2; PISP: 4.9.2	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2.1

Assessment Objective

Determine if the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-2(FIS-1) – Enhancement (Low)

Control

Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.

Applicability: All	**References:** FISCAM: TSC-2.4.4	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2(FIS-1).1

Assessment Objective

Determine if the organization accommodates regular and a reasonable amount of unscheduled maintenance in its data processing operations.

Assessment Methods And Objects

Examine: Maintenance documentation.

Examine: Pertinent policies and procedures.

Interview: Data processing and user management.

MA-2(FIS-2) – Enhancement (Low)

Control

Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users thus allowing for adequate testing. Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.

Applicability: All	**References:** FISCAM: TSC-2.4.10, TSC-2.4.11	**Related Controls:**

ASSESSMENT PROCEDURE: MA-2(FIS-2).1

Assessment Objective

Determine if:

(i) the organization schedules hardware equipment and related software changes such to minimize user impact and maximize resources for adequate testing; and

(ii) the organizational advance notification for hardware equipment changes does not cause unexpected interrupted user services.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation.

Interview: Senior management, data processing management, and user management.

MA-3 – Maintenance Tools (Low)

Control

The use of system maintenance tools, including diagnostic and test equipment and administration utilities, shall be approved, controlled, and monitored. Approved tools shall be maintained on an on-going basis.

Guidance

The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Applicability: All	**References:** ARS: MA-3; IRS-1075: 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-3; PISP: 4.9.3	**Related Controls:**

ASSESSMENT PROCEDURE: MA-3.1

Assessment Objective

Determine if:
(i) the organization approves, controls, and monitors the use of information system maintenance tools; and
(ii) the organization maintains maintenance tools on an ongoing basis.

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.(Optional)

MA-4 – Remote Maintenance (Low)

Control

Remote maintenance of a CMS information system must be approved by the CIO or his/her designated representative. Remote maintenance procedures shall be developed, documented, and implemented effectively to provide additional controls on remotely executed maintenance and diagnostic activities.

The use of remote diagnostic tools shall be described in the SSP for the information system. Maintenance records for all remote maintenance, diagnostic, and service activities shall be maintained and shall be reviewed periodically by appropriate organization officials. All sessions and remote connections shall be terminated after the remote maintenance is completed. If password-based authentication is used during remote maintenance, the passwords shall be changed following each remote maintenance service.

Guidance

Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST SP 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Applicability: All	**References:** ARS: MA-4; FISCAM: TAC-2.1.3; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4; PISP: 4.9.4	**Related Controls:** IA-2, MP-6

ASSESSMENT PROCEDURE: MA-4.1

Assessment Objective

Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-4(CMS-1) – Enhancement (Low)

Control

If remote maintenance is authorized in writing by the CIO or his/her designated representative:
Encrypt and decrypt diagnostic communications; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, terminate all sessions and remote connections. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.

Applicability: All	**References:** ARS: MA-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-4(CMS-1).1

Assessment Objective

Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that remote maintenance is authorized in writing by the CIO or his/her designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service.

Interview: Organizational personnel with information system maintenance responsibilities to determine that remote maintenance is authorized in writing by the CIO or his/her designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service.

MA-5 – Maintenance Personnel (Low)

Control

Maintenance personnel procedures shall be developed, documented, and implemented effectively to control maintenance of CMS information systems. A list of individuals authorized to perform maintenance on the information system shall be maintained.

Guidance

Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Applicability: All	**References:** ARS: MA-5; NIST 800-53/53A: MA-5; PISP: 4.9.5	**Related Controls:**

ASSESSMENT PROCEDURE: MA-5.1

Assessment Objective

Determine if the organization allows only authorized personnel to perform maintenance on the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-5(0) – Enhancement (Low)

Control

Only authorized individuals are allowed to perform maintenance. Ensure maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. Supervise maintenance personnel during the performance of maintenance activities when they do not have the needed access authorizations.

Applicability: All	**References:** ARS: MA-5(0); HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: MA-5; PISP: 4.9.5	**Related Controls:**

ASSESSMENT PROCEDURE: MA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-CMS-1 – Off-site Physical Repair of Systems (Low)

Control

Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality.

Guidance

It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approved Change Management baseline.

Storage media control when encrypted may take special considerations.

Applicability: All	**References:** ARS: MA-CMS-1; PISP: 4.9.7	**Related Controls:** AC-19(CMS-1), AC-3,

		CP-9, SC-12(CMS-1)

ASSESSMENT PROCEDURE: MA-CMS-1.1

Assessment Objective

Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair.

Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.

MA-CMS-1(CMS-0) – Enhancement (Low)

Control

Access to system for repair must be by authorized personnel only. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, check security features to verify they are functioning properly.

Applicability: All	**References:** ARS: MA-CMS-1(CMS-0); HIPAA: 164.310(d)(2)(i)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-CMS-1(CMS-0).1

Assessment Objective

Determine if the organization allows only authorized personnel perform maintenance on the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for repair. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, security features are checked to verify they are functioning properly.

Interview: Organizational personnel with information system maintenance responsibilities determine that only authorized personnel are permitted access to system for repair. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, security features are checked to verify they are functioning properly.

MA-CMS-2 – On-site Physical Repair of Systems (Low)

Control

Controls shall be developed, documented, and implemented effectively to enable on-site physical repair of systems without compromising security functionality or confidentiality.

Guidance

It is good practice to complete a full security review of a system before it is put back into operation when the system has completed repairs. The repaired system should match the approved Change Management baseline.

Storage media control when encrypted may take special considerations.

Applicability: All	**References:** ARS: MA-CMS-2; PISP: 4.9.8	**Related Controls:** AC-19(CMS-1), AC-3, CP-9, SC-12(CMS-1)

ASSESSMENT PROCEDURE: MA-CMS-2.1

Assessment Objective

Determine if the organization effectively develops procedures, documents procedures, and implements on-site repair of systems without compromising security functionality or confidentiality.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for on-site repair.

Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during on-site repair.

MA-CMS-2(CMS-1) – Enhancement (Low)

Control

Access to system for repair must be by authorized personnel only.

Applicability: All	**References:** ARS: MA-CMS-2(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: MA-CMS-2(CMS-1).1

Assessment Objective

Determine if the organization allows only authorized personnel perform maintenance on the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine physical repair of servers is performed within protected environments.

Interview: Organizational personnel with information system maintenance responsibilities to determine physical repair of servers is performed within protected environments.

Media Protection (MP) – *Operational*

MP-1 – Media Protection Policy and Procedures (Low)

Control

MP controls and procedures shall be developed, documented, and implemented effectively to address media access; media labeling; media transport; media destruction; media sanitization and clearing; media storage; and disposition of media records. The MP procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: MP-1; FISCAM: TAC-3.4; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1; NIST 800-53/53A: MP-1; PISP: 4.10.1	**Related Controls:**

ASSESSMENT PROCEDURE: MP-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents media protection policy and procedures;
(ii) the organization disseminates media protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review media protection policy and procedures; and
(iv) the organization updates media protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.(Optional)

ASSESSMENT PROCEDURE: MP-1.2

Assessment Objective

Determine if:
(i) the media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.(Optional)

MP-2 – Media Access (Low)

Control

Procedures shall be developed, documented, and implemented effectively to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media based on the sensitivity of the CMS information. Automated mechanisms shall be implemented to control access to media storage areas and to audit access attempts and access granted.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).
An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Applicability: All	**References:** ARS: MP-2; FISCAM: TAC-3.1.A.6, TAY-4.1.1; HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1; NIST 800-53/53A: MP-2; PISP: 4.10.2	**Related Controls:**

ASSESSMENT PROCEDURE: MP-2.1

Assessment Objective

Determine if the organization restricts access to information system media to authorized users.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records.

Interview: Organizational personnel with information system media protection responsibilities.(Optional)

MP-4 – Media Storage (Low)

Control

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper, within controlled areas. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security level of the information ever recorded on it until destroyed or sanitized using CMS-approved procedures.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management.

Applicability: All	**References:** ARS: MP-4; FISCAM: TCC-3.2.4, TCC-3.3.1; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1; NIST 800-53/53A: MP-4; PISP: 4.10.4	**Related Controls:** AC-19, CP-9, CP-9(4), RA-2, SC-7

ASSESSMENT PROCEDURE: MP-4.1

Assessment Objective

Determine if:

(i) the organization defines controlled areas for information system media;

(ii) the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk;

(iii) the organization defines the specific measures used to protect the selected media and information contained on that media;

(iv) the organization physically controls and securely stores information system media within controlled areas; and

(v) the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media; other relevant documents or records.(Optional)

MP-6 – Media Sanitization and Disposal (Low)

Control

Formal documented procedures shall be developed and implemented effectively to ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of data residing on storage devices, equipment, and hard copy documents. Media sanitization actions shall be tracked, documented, and verified. Sanitization equipment and procedures shall be tested periodically to ensure proper functionality.

Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmentally approved manner, to facilitate the disposal of media, both electronic

and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. Approved equipment removal procedures for CMS information systems and components that have processed or contained CMS information shall be followed. Inventory and disposition records for media, both electronic and paper, shall be produced, stored, updated, and retained.

Guidance

Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Applicability: All	**References:** ARS: MP-6; FISCAM: TAC-3.4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-1075: 4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2; NIST 800-53/53A: MP-6; PISP: 4.10.6	**Related Controls:** MA-4

ASSESSMENT PROCEDURE: MP-6.1

Assessment Objective

Determine if:

(i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process;

(ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and

(iii) information system media sanitation is consistent with NIST SP 800-88.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization records; audit records; other relevant documents or records.

Interview: Organizational personnel with information system media sanitization responsibilities.(Optional)

Physical and Environmental Protection (PE) – *Operational*

PE-1 – Physical and Environmental Protection Policy and Procedures (Low)

Control

Physical and environmental protection procedures shall be developed and implemented effectively to protect all CMS IT infrastructure and assets from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional. These procedures shall meet all federal, state and local building codes and be consistent with General Services Administration policies, directives, regulations, and guidelines.

Guidance

The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: PE-1; FISCAM: TSC-2.2.6, TSC-2.3.4, TSD-2.1; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1; NIST 800-53/53A: PE-1; PISP: 4.11.1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents physical and environmental protection policy and procedures;
(ii) the organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review physical and environmental protection policy and procedures; and
(iv) the organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Physical and environmental protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with physical and environmental protection responsibilities.(Optional)

ASSESSMENT PROCEDURE: PE-1.2

Assessment Objective

Determine if:
(i) the physical and environmental protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Physical and environmental protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with physical and environmental protection responsibilities.(Optional)

PE-1(FIS-1) – Enhancement (Low)

Control

Eating, drinking, and other behavior that may damage computer equipment is prohibited.

Applicability: All	**References:** FISCAM: TSC-2.2.7	**Related Controls:**

ASSESSMENT PROCEDURE: PE-1(FIS-1).1

Assessment Objective

Determine if the organization prohibits eating, drinking, and other behavior that may damage computer equipment.

Assessment Methods And Objects

Examine: Employee behavior.
Examine: Employee rules of behavior.
Examine: Pertinent policies and procedures.
Interview: Information system management and users.

PE-2 – Physical Access Authorizations (Low)

Control

Access lists of personnel with authorized access to facilities containing CMS information or information systems (except for those areas within the facilities officially designated as publicly accessible) shall be documented on standard forms, maintained on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessary, updated. Appropriate authorization credentials (e.g., badges, identification cards, smart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be removed promptly from all access lists.

Guidance

Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides.

Applicability: All	**References:** ARS: PE-2; FISCAM: TAC-2.1.1, TAC-2.1.2, TAC-2.1.4, TAC-2.2, TAC-3.1.A.3, TAC-3.1.A.4, TAC-3.1.A.8, TSS-1.2.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	**Related Controls:**

ASSESSMENT PROCEDURE: PE-2.1

Assessment Objective

Determine if:
(i) the organization identifies areas within the facility that are publicly accessible;
(ii) the organization defines the frequency of review and approval for the physical access list and authorization credentials for the facility;
(iii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
(iv) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and
(v) designated officials within the organization review and approve the access list and authorization credentials at the organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records.

PE-2(0) – Enhancement (Low)

Control

Review and approve lists of personnel with authorized access to facilities containing information systems at least once every 365 days.

Applicability: All	**References:** ARS: PE-2(0); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-3.1.A.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	**Related Controls:**

ASSESSMENT PROCEDURE: PE-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records.

PE-3 – Physical Access Control (Low)

Control

Physical access control devices (e.g., keys, locks, combinations, card-readers) and/or guards shall be used to control entry to and exit from facilities containing CMS information or information systems, except for areas and/or facilities officially designated as publicly accessible. Individual access authorizations shall be verified before granting access to facilities containing CMS information or information systems. Physical access control devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis.

Combinations, access codes, and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry to facilities during emergency-related events shall be restricted to authorized individuals only. Access to workstations and associated peripheral computing devices shall be appropriately controlled when located in areas designated as publicly accessible.

Guidance

The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73. If the token-based access control function employs cryptographic

verification, the access control system conforms to the requirements of NIST SP 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST SP 800-76.

Applicability: All	References: ARS: PE-3; FISCAM: TAC-3.1.A.3, TAC-3.1.A.5, TAC-3.1.A.7, TAC-3.1.A.8, TAC-3.1.B.2, TAN-2.1.1, TAN-2.1.2, TAN-2.2.1, TSD-2.1; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1; NIST 800-53/53A: PE-3; PISP: 4.11.3	Related Controls:

ASSESSMENT PROCEDURE: PE-3.1

Assessment Objective

Determine if:
(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
(ii) the organization verifies individual access authorizations before granting access to the facility; and
(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records.
Interview: Organizational personnel with physical access control responsibilities.(Optional)
Test: Physical access control capability.(Optional)

ASSESSMENT PROCEDURE: PE-3.2

Assessment Objective

Determine if:
(i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis;
(ii) the organization secures keys, combinations and other access devices on a regular basis; and
(iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records.
Test: Physical access control devices.(Optional)

ASSESSMENT PROCEDURE: PE-3.3

Assessment Objective

Determine if:
(i) the access control system is consistent with FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed);
(ii) the access control system is consistent with NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and
(iii) the access control system is consistent with NIST SP 800-76 (where the token-based access control function employs biometric verification).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST SP 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records.
Test: Physical access control devices.(Optional)

PE-3(CMS-1) – Enhancement (Low)

Control

Control data center / facility access by use of door and window locks.

Applicability: All	References: ARS: PE-3(CMS-1); IRS-1075: 4.6#1	Related Controls:

ASSESSMENT PROCEDURE: PE-3(CMS-1).1

Assessment Objective

Determine if the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine data center / facility access is controlled by use of door and window locks.

Interview: Organizational personnel with physical access control responsibilities to confirm data center / facility access is controlled by use of door and window locks.

PE-3(CMS-2) – Enhancement (Low)

Control

Store and operate servers in physically secure environments protected from unauthorized access.

Applicability: All	**References:** ARS: PE-3(CMS-2); FISCAM: TAC-3.1.A.5; IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-2).1

Assessment Objective

Determine if the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine servers are stored and operated in physically secure environments protected from unauthorized access.

Interview: Organizational personnel with physical access control responsibilities to determine servers are stored and operated in physically secure environments protected from unauthorized access.

PE-3(CMS-3) – Enhancement (Low)

Control

Data centers must meet the minimum requirements as established by the Federal Information Systems Control Audit Manual (FISCAM).

Applicability: All	**References:** ARS: PE-3(CMS-3); FISCAM: TAC-3.1.A.1, TAN-2.1.1, TAN-2.1.2; IRS-1075: 4.6#1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(CMS-3).1

Assessment Objective

Determine if:

(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

(ii) the organization verifies individual access authorizations before granting access to the facility; and

(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if data centers meet the minimum requirements as established by the Federal Information Systems Control Audit Manual (FISCAM).

PE-3(DIR-1) – Enhancement (Low)

Control

Controls are established to protect access authorization lists to secure areas such as data centers.

Applicability: All	**References:**	**Related Controls:**

ASSESSMENT PROCEDURE: PE-3(DIR-1).1

Assessment Objective

Determine if the organization protects approved access authorization lists that are for secure areas.

Assessment Methods And Objects

Examine: Protection procedures are in place for approved access authorization lists to secure areas.

PE-4 – Access Control for Transmission Medium (Low)

Control

Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering of CMS information system transmission lines within organizational facilities that carry unencrypted information.

Guidance

Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Applicability: All	**References:** ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4	**Related Controls:**

ASSESSMENT PROCEDURE: PE-4.1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records.(Optional)

PE-4(CMS-1) – Enhancement (Low)

Control

Prohibit public access to telephone closets and information system distribution and transmission lines within organizational facilities.

Applicability: All	**References:** ARS: PE-4(CMS-1); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: PE-4(CMS-1).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

Interview: Organizational personnel with physical access control responsibilities to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

PE-4(CMS-2) – Enhancement (Low)

Control

Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use.

Applicability: All	**References:** ARS: PE-4(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-4(CMS-2).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

Interview: Organizational personnel with physical access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

PE-6 – Monitoring Physical Access (Low)

Control

Physical access to information systems shall be monitored for physical security compliance and to detect and respond to incidents. Appropriate organization officials shall periodically review physical access records, investigate apparent security violations or suspicious physical access activities, and take appropriate remedial action.

Guidance

The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.

Applicability: All	**References:** ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN-2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6	**Related Controls:** IR-4

ASSESSMENT PROCEDURE: PE-6.1

Assessment Objective

Determine if the organization monitors physical access to the information system to detect and respond to physical security incidents.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; other relevant documents or records.

Interview: Organizational personnel with physical access monitoring responsibilities.(Optional)

Test: Physical access monitoring capability.(Optional)

PE-7 – Visitor Control (Low)

Control

Visitor controls shall be developed, documented, and implemented effectively to control access to sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries. Visitors shall be authenticated prior to being granted access to facilities or areas other than areas designated as publicly accessible. Government contractors and others with permanent authorization credentials are not considered visitors.

Guidance

Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST SP 800-79.

Applicability: All	**References:** ARS: PE-7; FISCAM: TAC-3.1.B.3; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7; PISP: 4.11.7	**Related Controls:**

ASSESSMENT PROCEDURE: PE-7.1

Assessment Objective

Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.
Interview: Organizational personnel with visitor access control responsibilities.(Optional)
Test: Visitor access control capability.(Optional)

PE-7(FIS-1) – Enhancement (Low)

Control

Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.

Applicability: All	**References:** FISCAM: TAC-3.1.B.3	**Related Controls:**

ASSESSMENT PROCEDURE: PE-7(FIS-1).1

Assessment Objective

Determine if the organization authenticates visitors, contractors and maintenance personnel through the use of preplanned appointments and identification checks.

Assessment Methods And Objects

Examine: Appointment and verification procedures for visitors.
Examine: Pertinent policies and procedures.
Interview: Receptionist or security guard.

PE-8 – Access Records (Low)

Control

Visitor access to sensitive facilities and restricted / controlled areas that contain CMS information or information systems shall be logged. The visitor access record shall contain:
4.11.8.1. Name and organization of the person visiting;
4.11.8.2. Signature of the visitor;
4.11.8.3. Form of identification;
4.11.8.4. Date of access;
4.11.8.5. Time of entry and departure;
4.11.8.6. Purpose of visit; and
4.11.8.7. Name and organization of person visited.

Appropriate organization officials shall periodically review the access records, including after closeout.

Guidance

It is good practice to have a standard log format for consistency and ease of use during log closeouts and the next months log generation.

Applicability: All	**References:** ARS: PE-8; FISCAM: TAC-3.1.B.1, TAC-3.1.B.3; NIST 800-53/53A: PE-8; PISP: 4.11.8	**Related Controls:**

ASSESSMENT PROCEDURE: PE-8.1

Assessment Objective

Determine if:

(i) the organization defines the frequency of review for visitor access records;
(ii) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes:
- name and organization of the person visiting;
- signature of the visitor;
- form of identification;
- date of access;
- time of entry and departure;
- purpose of visit;
- name and organization of person visited and

(iii) designated officials within the organization review the visitor access logs in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan; facility access control records; other relevant documents or records.

PE-8(0) – Enhancement (Low)

Control

Visitor access records must be closed out and reviewed by management monthly.

Applicability: All	**References:** ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8	**Related Controls:**

ASSESSMENT PROCEDURE: PE-8(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan (for organization-defined frequency for review of visitor access records); facility access control records; other relevant documents or records.

PE-9 – Power Equipment and Power Cabling (Low)

Control

Power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain safe power for CMS information systems.

Guidance

Both primary and backup power systems should be included in the safe power implementation procedures. Remote backup site's power implementation should be included in the documentation.

Applicability: All	**References:** ARS: PE-9; NIST 800-53/53A: PE-9; PISP: 4.11.9	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9.1

Assessment Objective

Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.(Optional)

PE-9(CMS-1) – Enhancement (Low)

Control

Prohibit public access to infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

Applicability: All	**References:** ARS: PE-9(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9(CMS-1).1

Assessment Objective

Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

Interview: Organizational personnel with physical access control responsibilities to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power

generators, HVAC systems, cabling, and wiring closets.

PE-9(CMS-2) – Enhancement (Low)

Control

Power surge protection must be implemented for all computer equipment.

Applicability: All	**References:** ARS: PE-9(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-9(CMS-2).1

Assessment Objective

Determine if the organization protects power equipment and implements surge protection for all computers to assist in protection from damage or destruction.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents /records / diagrams to determine if power surge protection is implemented for all computer equipment.

Interview: Organizational personnel with physical access control responsibilities to determine if power surge protection is implemented for all computer equipment.

PE-11 – Emergency Power (Low)

Control

Emergency power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to facilitate an orderly shutdown of the CMS information system in the event of a primary power source loss.

Guidance

Both primary and backup processing locations should be included in the safe power implementation procedures. The remote backup site's power implementation should be included in the documentation. Even though unlikely that both the primary and backup locations will be switching to emergency power at the same time, it is prudent to minimize the risk to a total lose of a processing capability.

Applicability: All	**References:** ARS: PE-11; FISCAM: TSC-2.2.5; NIST 800-53/53A: PE-11; PISP: 4.11.11	**Related Controls:**

ASSESSMENT PROCEDURE: PE-11.1

Assessment Objective

Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records.(Optional)

Test: Uninterruptible power supply.(Optional)

PE-12 – Emergency Lighting (Low)

Control

Mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enhance safety and availability. Automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes shall be provided.

Guidance

Local building safety codes are a good place to obtain the needed information for documenting emergency lighting implementation procedures and architecture.

Applicability: All	**References:** ARS: PE-12; NIST 800-53/53A: PE-12; PISP: 4.11.12	**Related Controls:**

ASSESSMENT PROCEDURE: PE-12.1

Assessment Objective

Determine if:

(i) the organization employs and maintains automatic emergency lighting systems that activates in the event of a power outage or disruption; and

(ii) the organization employs and maintains automatic emergency lighting systems that cover emergency exits and evacuation routes.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records.

Test: Emergency lighting capability.(Optional)

PE-13 – Fire Protection (Low)

Control

Fire protection mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to prevent, detect, and respond to fire. Fire suppression and

detection devices / systems that can be activated in the event of a fire shall be employed and maintained. Fire suppression and detection devices / systems shall include, but not be limited to, sprinkler systems, hand-held fire extinguishers, fixed fire hoses, and smoke detectors.

Guidance

Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Applicability: All	**References:** ARS: PE-13; FISCAM: TSC-2.2.1, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-13; PISP: 4.11.13	**Related Controls:**

ASSESSMENT PROCEDURE: PE-13.1

Assessment Objective

Determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records.

PE-14 – Temperature and Humidity Controls (Low)

Control

Temperature and humidity control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain (within acceptable levels) and monitor the temperature and humidity of facilities containing CMS information systems.

Guidance

Local building a safety codes are a good place to obtain the needed information for documenting HVAC implementation procedures and architecture. Consideration for Occupational Safety and Health Administration (OSHA) requirements maybe included.

Applicability: All	**References:** ARS: PE-14; FISCAM: TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-14; PISP: 4.11.14	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14.1

Assessment Objective

Determine if:
(i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and
(ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records.

PE-14(CMS-1) – Enhancement (Low)

Control

Evaluate the level of alert and follow prescribed guidelines for that alert level.

Applicability: All	**References:** ARS: PE-14(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(CMS-1).1

Assessment Objective

Determine if:
(i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and
(ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records to determine the level of alert and prescribed guidelines for that alert level.
Interview: Organizational personnel with environmental protection responsibilities to determine if there exists the level of alert and prescribed guidelines for that alert level.

PE-14(FIS-1) – Enhancement (Low)

Control

Redundancy exists in the air cooling system.

Applicability: All	**References:** FISCAM: TSC-2.2.3	**Related Controls:**

ASSESSMENT PROCEDURE: PE-14(FIS-1).1

Assessment Objective

Determine if the organization uses redundant air cooling systems.

Assessment Methods And Objects

Examine: Entity's facilities.
Examine: Operation, location, maintenance, and access to the air cooling systems.
Examine: Pertinent policies and procedures.
Interview: Site manager.

PE-15 – Water Damage Protection (Low)

Control

All necessary steps shall be taken to ensure that the building plumbing does not endanger CMS information systems. Procedures shall be developed, documented, and implemented effectively to reduce the potential damage from plumbing leaks.

Guidance

Local building a safety codes are a good place to obtain the needed information for documenting water damage protection procedures and architecture. Consideration for Occupational Safety and Health Administration (OSHA) requirements maybe included.

Applicability: All	**References:** ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15; PISP: 4.11.15	**Related Controls:**

ASSESSMENT PROCEDURE: PE-15.1

Assessment Objective

Determine if:
(i) the organization identifies key personnel with knowledge of location and operational procedures for activating master shutoff valves for plumbing system; and
(ii) the organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff values; list of key personnel with knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value documentation; other relevant documents or records.
Interview: Organization personnel with physical and environmental protection responsibilities.(Optional)
Test: Simulated master water shutoff value activation for the plumbing system.(Optional)

PE-16 – Delivery and Removal (Low)

Control

Procedures shall be developed, documented, and implemented effectively to control the flow of information system-related items into and out of the organization. Appropriate officials shall authorize the delivery or removal of CMS information system-related items.

To avoid unauthorized access, delivery and removal controls shall be implemented to isolate delivery areas from sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries.

Guidance

The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.

Applicability: All	**References:** ARS: PE-16; NIST 800-53/53A: PE-16; PISP: 4.11.16	**Related Controls:**

ASSESSMENT PROCEDURE: PE-16.1

Assessment Objective

Determine if:
(i) the organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility; and
(ii) the organization maintains appropriate records of items entering and exiting the facility.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records.
Interview: Organization personnel with tracking responsibilities for information system components entering and exiting the facility.(Optional)

PE-17 – Alternate Work Site (Low)		
Control Procedures shall be developed, documented, and implemented effectively to control information system security at alternate work sites. A method of communication shall be provided to employees at alternate work sites to report security issues or suspected security incidents.		
Guidance The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST SP 800-46 provides guidance on security in telecommuting and broadband communications.		
Applicability: All	**References:** ARS: PE-17; HIPAA: 164.310(a)(2)(i); NIST 800-53/53A: PE-17; PISP: 4.11.17	**Related Controls:**
ASSESSMENT PROCEDURE: PE-17.1		
Assessment Objective Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites. **Assessment Methods And Objects** **Examine:** Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records.(Optional) **Interview:** Organization personnel using alternate work sites.(Optional)		

Planning (PL) – *Management*

PL-1 – Security Planning Policy and Procedures (Low)

Control

All CMS information systems and major applications shall be documented in a SSP, which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, in accordance with current CMS Procedures.

Guidance

The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-18 provides guidance on security planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: PL-1; FISCAM: TSP-2.1, TSP-3.2; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2; NIST 800-53/53A: PL-1; PISP: 4.12.1	**Related Controls:**

ASSESSMENT PROCEDURE: PL-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security planning policy and procedures;
(ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review security planning policy and procedures; and
(iv) the organization updates security planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: PL-1.2

Assessment Objective

Determine if:
(i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

PL-1(FIS-1) – Enhancement (Low)

Control

Security policies are distributed to all affected personnel.

Applicability: All	**References:** FISCAM: TSP-3.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-1(FIS-1).1

Assessment Objective

Determine if the organization distributes security policies to all affected personnel.

Assessment Methods And Objects

Examine: Memos, electronic mail files, or other policy distribution mechanisms.
Interview: Staff and system users to determine how security policies are distributed.

PL-2 – System Security Plan (SSP) (Low)

Control

All CMS information systems and major applications shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18. The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization

officials and incorporated into the information resources management strategic plan. The information contained in the SSP is subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The security plan is aligned with the organization's information system architecture and information security architecture. NIST SP 800-18 provides guidance on security planning.

Applicability: All	**References:** ARS: PL-2; FISCAM: TAC-3.1.A.1, TSP-2.1, TSP-3.2; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3; NIST 800-53/53A: PL-2; PISP: 4.12.2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2.1

Assessment Objective

Determine if:
(i) the organization develops and implements a security plan for the information system;
(ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements;
(iii) the security plan development is consistent with NIST SP 800-18 and the concepts in the NIST Risk Management Framework including baseline security control selection, tailoring of the baseline, and supplementation of the tailored baseline;
(iv) the security plan is consistent with the organization's information system architecture and information security architecture; and
(v) designated organizational officials review and approve the security plan.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan development and implementation; NIST SP 800-18; security plan for the information system; other relevant documents or records.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

PL-2(CMS-1) – Enhancement (Low)

Control

Document the in-place security controls of the system according to the CMS System Security Plan (SSP) Procedures.

Applicability: All	**References:** ARS: PL-2(CMS-1); FISCAM: TSP-2.1; HIPAA: 164.316(b)(1)(i), 164.316(b)(1)(ii); HSPD 7: J(35); IRS-1075: 4.7.3#2	**Related Controls:**

ASSESSMENT PROCEDURE: PL-2(CMS-1).1

Assessment Objective

Determine if:
(i) the organization develops and implements a security plan for the information system;
(ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements;
(iii) the security plan is consistent with NIST SP 800-18;
(iv) the security plan is consistent with the organization's information system architecture and information security architecture; and
(v) designated organizational officials review and approve the security plan.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan development and implementation; NIST SP 800-18; security plan for the information system; other relevant documents or records to determine the in-place security controls of the system are documented according to the CMS System Security Plan (SSP) Procedures.
Interview: Organizational personnel with information system security planning and plan implementation responsibilities to determine if System Security Plan (SSP) includes the in-place security controls of the system and are documented according to the CMS System Security Plan (SSP) Procedures.

PL-3 – System Security Plan Update (Low)

Control

The SSP shall be reviewed at least every 365 days and updated minimally every three (3) years to reflect current conditions or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security; when the data sensitivity level increases; after a serious security violation; due to changes in the threat environment; or before the previous accreditation expires.

Guidance

Significant changes are defined in advance by the organization and identified in the configuration management process. NIST SP 800-18 provides guidance on security plan updates.

Applicability: All	**References:** ARS: PL-3; FISCAM: TSP-2.2; HIPAA: 164.306(a)(3), 164.316(a), 164.316(b)(2)(iii); HSPD 7: G(24), J(35); IRS-1075: 5.6.1.2#1.4; NIST 800-53/53A: PL-3; PISP: 4.12.3	**Related Controls:**

ASSESSMENT PROCEDURE: PL-3.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of information system security plan reviews and updates;
(ii) the organization updates the security plan in accordance with organization-defined frequency, at least annually;
(iii) the organization receives input to update the security plan from the organization's configuration management and control process; and
(iv) the updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan updates; information system security plan; configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records.

PL-4 – Rules of Behavior (ROB) (Low)

Control

ROBs shall be established, and made readily available, to delineate clearly user responsibilities and expected behavior of all Business Owners, users, operators, and administrators with regard to information and information system usage. Before authorizing access to the information system and / or information and annually thereafter, the organization shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the ROBs. Specific ROBs shall be established to govern work-at-home users who access CMS information or information systems.

Limited personal use of organization-owned or leased equipment and resources shall be considered to be a permitted use of organization-owned or leased equipment and resources when the following conditions are met:
4.12.4.1. Such use involves minimal additional expense to CMS;
4.12.4.2. Such use does not interfere with the mission or operation of CMS;
4.12.4.3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch;
4.12.4.4. Such use does not overburden any CMS information system resources;
4.12.4.5. Such use is not otherwise prohibited under this policy; and
4.12.4.6. Any use of organizational Internet and email resources shall be made with the understanding that such use is not secure, private or anonymous.

The following uses of organization-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited:
4.12.4.7. Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace;
4.12.4.8. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords;
4.12.4.9. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity;
4.12.4.10. All email communications to groups of employees that are subject to approval prior to distribution and have not been approved by the organization (e.g., retirement announcements, union notices or announcements, charitable solicitations); and
4.12.4.11. Employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees.

All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of organization-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that employees desire to protect their privacy, employees shall not use organization-owned or leased equipment and resources.

Guidance

Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST SP 800-18 provides guidance on preparing rules of behavior.

Applicability: All	**References:** ARS: PL-4; FISCAM: TSP-3.3.2; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.5; NIST 800-53/53A: PL-4; PISP: 4.12.4	**Related Controls:**

ASSESSMENT PROCEDURE: PL-4.1

Assessment Objective

Determine if:
(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;
(ii) the organization makes the rules available to all information system users;
(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and
(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records.

Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior.(Optional)

PL-4(CMS-1) – Enhancement (Low)

Control

Define user roles and expectations for system and network use.

Applicability: All	**References:** ARS: PL-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-4(CMS-1).1

Assessment Objective

Determine if:

(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;

(ii) the organization makes the rules available to all information system users;

(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and

(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records to determine user roles and expectations for system and network use are defined.

Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior to determine user roles and expectations for system and network use are defined.

PL-4(CMS-2) – Enhancement (Low)

Control

Electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

Applicability: All	**References:** ARS: PL-4(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: PL-4(CMS-2).1

Assessment Objective

Determine if:

(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;

(ii) the organization makes the rules available to all information system users;

(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and

(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records to determine electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior to determine electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

PL-5 – Privacy Impact Assessment (PIA) (Low)

Control

PIAs shall be conducted for CMS information systems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandum M-03-22, and the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations.

Guidance

OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

Applicability: All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC	**References:** ARS: PL-5; HSPD 7: J(35); NIST 800-53/53A: PL-5; PISP: 4.12.5	**Related Controls:**

ASSESSMENT PROCEDURE: PL-5.1

Assessment Objective

Determine if:
(i) the organization conducts a privacy impact assessment on the information system in accordance with OMB policy; and
(ii) the privacy impact assessment is consistent with federal legislation and OMB policy.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing privacy impact assessments on the information system; appropriate federal legislation and OMB policy; privacy impact assessment; other relevant documents or records.

PL-6 – Security-Related Activity Planning (Low)

Control

Security-related activities affecting the information system shall be planned and coordinated before being performed in order to reduce the impact on CMS operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing / exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Guidance

Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Applicability: All	**References:** ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6	**Related Controls:**

ASSESSMENT PROCEDURE: PL-6.1

Assessment Objective

Determine if:
(i) the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations, organizational assets, and individuals; and
(ii) the organization's advance planning and coordination of security-related activities includes both emergency and non-emergency situations.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records.(Optional)
Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

Personnel Security (PS) – *Operational*

PS-1 – Personnel Security Policy and Procedures (Low)		
Control CMS information systems shall employ personnel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines. Procedures shall be developed to guide the implementation of personnel security controls.		
Guidance The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.		
Applicability: All	**References:** ARS: PS-1; FISCAM: TSD-1.3.3; IRS-1075: 5.6.2.1#1.1-2; NIST 800-53/53A: PS-1; PISP: 4.13.1	**Related Controls:**
ASSESSMENT PROCEDURE: PS-1.1		
Assessment Objective Determine if: (i) the organization develops and documents personnel security policy and procedures; (ii) the organization disseminates personnel security policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review personnel security policy and procedures; and (iv) the organization updates personnel security policy and procedures when organizational review indicates updates are required. **Assessment Methods And Objects** **Examine:** Personnel security policy and procedures, other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.(Optional)		
ASSESSMENT PROCEDURE: PS-1.2		
Assessment Objective Determine if: (i) the personnel security policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the personnel security policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the personnel security procedures address all areas identified in the personnel security policy and address achieving policy-compliant implementations of all associated security controls. **Assessment Methods And Objects** **Examine:** Personnel security policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.(Optional)		
PS-1(FIS-1) – Enhancement (Low)		
Control Staff's performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.		
Applicability: All	**References:** FISCAM: TSD-2.2.1	**Related Controls:**
ASSESSMENT PROCEDURE: PS-1(FIS-1).1		
Assessment Objective Determine if the organization monitors staff performance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are carried out. **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes). **Interview:** Management and subordinate personnel.		
PS-1(FIS-2) – Enhancement (Low)		
Control Regularly scheduled vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.		
Applicability: All	**References:** FISCAM: TSD-1.1.7, TSP-4.1.4, TSP-4.1.5	**Related Controls:**

ASSESSMENT PROCEDURE: PS-1(FIS-2).1

Assessment Objective

Determine if the organization regularly schedules vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.

Assessment Methods And Objects

Examine: Personnel records to identify individuals who have not taken vacation or sick leave in the past year.
Examine: Staff assignment records and determine whether job and shift rotations occur.
Examine: Vacation and job rotation policies and procedures.
Interview: Information system management and users.

PS-1(FIS-3) – Enhancement (Low)

Control

Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes. Employees are made aware of their job descriptions.

Applicability: All	**References:** FISCAM: TSD-1.2.2, TSD-1.3.1, TSP-4.2.1, TSS-2.1.2, TSS-2.1.3	**Related Controls:**

ASSESSMENT PROCEDURE: PS-1(FIS-3).1

Assessment Objective

Determine if:
(i) the organizational documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes.
(ii) the organization makes the employees aware of their job descriptions.

Assessment Methods And Objects

Examine: Effective dates of the position descriptions and determine whether they are current.
Examine: Job descriptions for several positions in organizational units and for user security administrators.
Examine: Job descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
Interview: Management personnel.

PS-2 – Position Categorization (Low)

Control

A criticality / sensitivity rating (e.g., non-sensitive, national security, public trust) shall be assigned to all positions within the organization. The criticality / sensitivity rating shall be in compliance with 5 CFR 731.106(a), Executive Orders 10450 and 12968, NSPD-1, HSPD-7, and HSPD-12 and consistent with OPM policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating. All criticality / sensitivity ratings must be submitted to the DHHS HR department and CMS' personnel security department.

Guidance

Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Applicability: All	**References:** ARS: PS-2; IRS-1075: 5.6.2.1#1.3; NIST 800-53/53A: PS-2; PISP: 4.13.2	**Related Controls:**

ASSESSMENT PROCEDURE: PS-2.1

Assessment Objective

Determine if:
(i) the organization assigns a risk designations to all positions within the organization;
(ii) the organization establishes a screening criteria for individuals filling organizational positions;
(iii) the risk designations for the organizational positions are consistent with applicable federal regulations and OPM policy and guidance;
(iv) the organization defines the frequency of risk designation reviews and updates for organizational positions; and
(v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan; records of risk designation reviews and updates; other relevant documents or records.

PS-2(0) – Enhancement (Low)

Control

Review and revise position risk designations every 365 days.

Applicability: All	References: ARS: PS-2(0); NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:

ASSESSMENT PROCEDURE: PS-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan (for organization-defined frequency for review of position categorizations); records of risk designation reviews and updates; other relevant documents or records.

PS-3 – Personnel Screening (Low)

Control

Prior to being granted access, all employees and contractors who require access to CMS information or information systems shall be screened and reinvestigated periodically, consistent with the criticality / sensitivity rating of the position. For prospective employees, references background checks shall be performed before issuance of a User ID. Security agreements shall be required for employees and contractors assigned to work with mission critical information.

Guidance

Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and SP 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.

Applicability: All	References: ARS: PS-3; FISCAM: TSP-4.1.1, TSP-4.1.2; IRS-1075: 5.6.2.1#1.4; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:

ASSESSMENT PROCEDURE: PS-3.1

Assessment Objective

Determine if:

(i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and

(ii) the personnel screening is consistent with appropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 800-78; other relevant documents or records.

PS-3(0) – Enhancement (Low)

Control

Perform criminal history check for all persons prior to employment.

Applicability: All	References: ARS: PS-3(0); FISCAM: TSP-4.1.2; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:

ASSESSMENT PROCEDURE: PS-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 800-78; other relevant documents or records.

PS-3(CMS-1) – Enhancement (Low)

Control

Require personnel to obtain and hold a low-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

Applicability: All	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:

ASSESSMENT PROCEDURE: PS-3(CMS-1).1

Assessment Objective

Determine if:

(i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and

(ii) the personnel screening is consistent with appropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; and other relevant documents or records to determine that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

Interview: Personnel with personnel screening responsibilities to confirm that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

PS-4 – Personnel Termination (Low)

Control

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information and information systems is removed upon personnel termination. Termination procedures shall address:

4.13.4.1. Exit interviews;
4.13.4.2. Retrieval of all organizational information system-related property;
4.13.4.3. Notification to security management;
4.13.4.4. Revocation of all system access privileges;
4.13.4.5. Immediately escorting employees terminated for cause out of organization facilities; and
4.13.4.6. Hard disk back up and sanitization before re-issuance.

Appropriate personnel shall have access to official records created by the terminated employee that are stored on organizational information systems.

Guidance

Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Applicability: All	**References:** ARS: PS-4; FISCAM: TAC-2.1.6, TSP-4.1.6; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: 5.6.2.1#1.5; NIST 800-53/53A: PS-4; PISP: 4.13.4	**Related Controls:**

ASSESSMENT PROCEDURE: PS-4.1

Assessment Objective

Determine if:
(i) the organization terminates information system access upon termination of individual employment;
(ii) the organization conducts exit interviews of terminated personnel;
(iii) the organization retrieves all organizational information system-related property from terminated personnel; and
(iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities.(Optional)

PS-4(CMS-1) – Enhancement (Low)

Control

Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination.

Applicability: All	**References:** ARS: PS-4(CMS-1); FISCAM: TAC-3.2.C.4	**Related Controls:**

ASSESSMENT PROCEDURE: PS-4(CMS-1).1

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

Interview: Personnel with termination responsibilities to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

PS-5 – Personnel Transfer (Low)

Control

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information or information systems no longer required in the new assignment is terminated upon personnel transfer. Transfer procedures shall address:

4.13.5.1. Re-issuing appropriate organizational information system-related property (e.g., keys, identification cards, building passes);
4.13.5.2. Notification to security management;
4.13.5.3. Closing obsolete accounts and establishing new accounts; and
4.13.5.4. Revocation of all system access privileges (if applicable).

Guidance

Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts.

Applicability: All	**References:** ARS: PS-5; FISCAM: TAC-2.1.6, TSP-4.1.6; IRS-1075: 5.6.2.1#1.6; NIST 800-53/53A: PS-5; PISP: 4.13.5	**Related Controls:**

ASSESSMENT PROCEDURE: PS-5.1

Assessment Objective

Determine if:
(i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and
(ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

PS-6 – Access Agreements (Low)

Control

Individuals who require access to CMS information or information systems shall be required to complete and sign appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements.

Guidance

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Applicability: All	**References:** ARS: PS-6; FISCAM: TSP-4.1.3; IRS-1075: 5.6.2.1#1.7; NIST 800-53/53A: PS-6; PISP: 4.13.6	**Related Controls:**

ASSESSMENT PROCEDURE: PS-6.1

Assessment Objective

Determine if:
(i) the organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access;
(ii) organizational personnel sign access agreements;
(iii) the organization defines the frequency of reviews and updates for access agreements; and
(iv) the organization reviews and updates the access agreements in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records.

PS-6(0) – Enhancement (Low)

Control

Access agreements are reviewed and updated as part of the system accreditation or when a contract is renewed or extended.

Applicability: All	**References:** ARS: PS-6(0); NIST 800-53/53A: PS-6; PISP: 4.13.6	**Related Controls:**

ASSESSMENT PROCEDURE: PS-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan (for organization-defined frequency for access agreement reviews); access agreements; records of access agreement reviews and updates; other relevant documents or records.

PS-7 – Third-Party Personnel Security (Low)

Control

Personnel security controls employed by external service providers and third parties shall be documented, agreed to, implemented effectively, and monitored for compliance and shall include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements. Personnel security controls employed by service providers and third parties shall be compliant with CMS IS policies and procedures, and consistent with NIST SP 800-35.

Guidance

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST SP 800-35 provides guidance on information technology security services.

Applicability: All	**References:** ARS: PS-7; IRS-1075: 5.6.2.1#1.8; NIST 800-53/53A: PS-7; PISP: 4.13.7	**Related Controls:**

ASSESSMENT PROCEDURE: PS-7.1

Assessment Objective

Determine if:
(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management);
(ii) the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST SP 800-35; and
(iii) the organization monitors third-party provider compliance with personnel security requirements.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities; third-party providers.(Optional)

PS-7(CMS-1) – Enhancement (Low)

Control

Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.

Applicability: All	**References:** ARS: PS-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: PS-7(CMS-1).1

Assessment Objective

Determine if:
(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management); and
(ii) the organization monitors third-party provider compliance with personnel security requirements.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records to determine the access provided to contractors and defining security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.
Interview: Personnel with third party security responsibilities to determine that the access provided to contractors are defined within the security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies, and standards.

PS-8 – Personnel Sanctions (Low)

Control

The organization shall enforce formal personnel sanctions process for personnel who fail to comply with established CMS IS policies and procedures. The employee sanction process shall be consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines.

Guidance

The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Applicability: All	**References:** ARS: PS-8; HIPAA: 164.308(a)(1)(ii)(C); NIST 800-53/53A: PS-8; PISP: 4.13.8	**Related Controls:**

ASSESSMENT PROCEDURE: PS-8.1

Assessment Objective

Determine if:
(i) the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
(ii) the personnel sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records.

PS-CMS-1 – Review System Access during Extraordinary Personnel Circumstances (Low)

Control

Access to CMS information and information systems shall be reviewed during extraordinary personnel circumstances and limited as deemed necessary.

Guidance

A death in the family or other personal problems could be considered extraordinary personal circumstances. For some personnel, recovery from a difficult time may take longer than usual and management must consider the circumstances on a case by case basis.

Applicability: All	**References:** ARS: PS-9; PISP: 4.13.9	**Related Controls:**

ASSESSMENT PROCEDURE: PS-CMS-1.1

Assessment Objective

Determine if the organization manages personnel with extraordinary personal circumstances.

Assessment Methods And Objects

Examine: Personnel security policy and procedures; other relevant documents or records determine system access during extraordinary personnel circumstances is reviewed and access is limited as deemed necessary.

Interview: Organizational personnel with personnel security responsibilities to determine system access during extraordinary personnel circumstances is reviewed and access is limited as deemed necessary.

PS-CMS-2 – Designate an Information System Security Officer (ISSO) / System Security Officer (SSO) (Low)

Control

An Information System Security Officer (ISSO) / System Security Officer (SSO) shall be designated for each business component with roles and responsibilities of the position clearly defined.

Guidance

A good reference set for defining the Information System Security Officer (ISSO) / System Security Officer (SSO) responsibilities are the NIST SPs. Specific responsibilities should be developed to protect CMS information systems and data.

Applicability: All	**References:** ARS: PS-10; FISCAM: TSP-3.1.1, TSP-3.1.2; HIPAA: 164.308(a)(2); PISP: 4.13.10	**Related Controls:**

ASSESSMENT PROCEDURE: PS-CMS-2.1

Assessment Objective

Determine if the organization has documented the roles and responsibilities of appointed ISSO / SSO.

Assessment Methods And Objects

Examine: Personnel security policy and procedures; other relevant documents or records to determine an ISSO / SSO is designated for each component with roles and responsibilities of the position clearly defined.

Interview: Organizational personnel with personnel security responsibilities to determine an ISSO / SSO is designated for each component with roles and responsibilities of the position clearly defined.

Risk Assessment (RA) – *Management*

RA-1 – Risk Assessment Policy and Procedures (Low)

Control

All CMS applications and systems shall be covered by an IS RA. The RA shall be consistent with NIST SP 800-30. Formal documented procedures shall be developed, disseminated, and reviewed / updated periodically to facilitate the implementation of the RA policy and associated RA controls. The procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-30 provides guidance on the assessment of risk. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: RA-1; FISCAM: TAC-3.1.A.2; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075: 5.6.1.1#1.1-2; NIST 800-53/53A: RA-1; PISP: 4.14.1	**Related Controls:**

ASSESSMENT PROCEDURE: RA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents risk assessment policy and procedures;
(ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review risk assessment policy and procedures; and
(iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.(Optional)

ASSESSMENT PROCEDURE: RA-1.2

Assessment Objective

Determine if:
(i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.(Optional)

RA-2 – Security Categorization (Low)

Control

CMS information systems and the information processed, stored, or transmitted by the systems shall be categorized in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to the, CMS System Security Level by Information Type. The security categorization (including supporting rationale) shall be explicitly documented. Designated senior-level officials within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the CMS CIO, CISO, and Business Owners.

All CMS information systems categorized as high or moderate shall be considered sensitive or to contain sensitive information. All CMS information systems categorized as low shall be considered non-sensitive or to contain non-sensitive information. All CMS information systems shall implement minimum security requirements and controls as established in the current CMS IS Standards, based on security categorization of the system.

Guidance

The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST SP 800-60 provides guidance on determining the security categories of the

information types resident on the information system.

Applicability: All	**References:** ARS: RA-2; FISCAM: TAC-1.1; HSPD 7: D(8); IRS-1075: 4.1#2; NIST 800-53/53A: RA-2; PISP: 4.14.2	**Related Controls:** MP-4, SC-7

ASSESSMENT PROCEDURE: RA-2.1

Assessment Objective

Determine if:
(i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners;
(ii) the security categorization is consistent with FIPS 199 and NIST SP 800-60;
(iii) the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts;
(iv) the organization includes supporting rationale for impact-level decisions as part of the security categorization; and
(v) designated, senior-level organizational officials review and approve the security categorization of the information system.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST SP 800-60; information system security plan; other relevant documents or records.
Interview: Organizational personnel with security categorization and risk assessment responsibilities.(Optional)

RA-3 – Risk Assessment (RA) (Low)

Control

An assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that support the operations and assets of CMS shall be performed, both within CMS and by external parties that manage / operate information or information systems for CMS. The RA shall be in accordance with current CMS Procedures. Based on the operation of the information system, the RA shall take into account vulnerabilities, threat sources, and security controls in place to determine the resulting level of residual risk posed to CMS operations, CMS assets, CMS information, or individuals.

Any findings from reviews of CMS systems shall be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses shall be documented by the Business Owner or external party and addressed by mitigating the risk, accepting the risk with explanation or submitting Corrective Action Plan (CAP). These findings shall be subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST SP 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Applicability: All	**References:** ARS: RA-3; FISCAM: TAC-3.1.A.2, TSP-1.1.2, TSP-1.1.3, TSP-5.1.4; HIPAA: 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3, 6.3.3#2; NIST 800-53/53A: RA-3; PISP: 4.14.3	**Related Controls:**

ASSESSMENT PROCEDURE: RA-3.1

Assessment Objective

Determine if:
(i) the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and
(ii) the risk assessment is consistent with the NIST SP 800-30.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST SP 800-30; other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.(Optional)

RA-3(CMS-1) – Enhancement (Low)

Control

Perform an IS RA for the system, and document the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

Applicability: All	**References:** ARS: RA-3(CMS-1); FISCAM: TAC-1.1, TAC-1.2, TSS-2.2.4; HIPAA: 164.306(a)(2); HSPD 7: D(8)	**Related Controls:**

ASSESSMENT PROCEDURE: RA-3(CMS-1).1

Assessment Objective

Determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties).

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; information system security plan (for organization-defined frequency for risk assessment updates); records of risk assessment updates; NIST SP 800-30; other relevant documents or records to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

Interview: Organizational personnel with risk assessment responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

RA-4 – Risk Assessment Update (Low)

Control

The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation.

Guidance

The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates.

Applicability: All	**References:** ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4	**Related Controls:**

ASSESSMENT PROCEDURE: RA-4.1

Assessment Objective

Determine if:

(i) the organization defines the frequency of risk assessment updates;

(ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system;

(iii) the risk assessment update is consistent with the NIST SP 800-30; and

(iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing risk assessment updates; risk assessment; information system security plan; records of risk assessment updates; NIST SP 800-30; other relevant documents or records.

RA-5 – Vulnerability Scanning (Low)

Control

Appropriate vulnerability assessment tools and techniques shall be implemented by the organization. Selected personnel shall be trained in their use and maintenance. The organization shall conduct periodic testing of its security posture by scanning its information systems with vulnerability tools. The information obtained from the vulnerability scanning process shall be shared with appropriate personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems. The activities of employees using organization Internet and email resources shall be subject to monitoring by system or security personnel without notice.

Guidance

Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST SP 800-42 provides guidance on

network security testing. NIST SP 800-40 (Version 2) provides guidance on patch and vulnerability management.

Applicability: All	References: ARS: RA-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5; PISP: 4.14.5	Related Controls:

ASSESSMENT PROCEDURE: RA-5.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of vulnerability scans within the information system;
(ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported;
(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact;
(iv) the organization performs network vulnerability scanning in accordance with NIST SP 800-42; and
(v) the organization handles patch and vulnerability management in accordance with NIST SP 800-40.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.(Optional)
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.(Optional)

RA-5(CMS-1) – Enhancement (Low)

Control

Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once a year, in accordance with CMS IS procedures. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.

Applicability: All	References: ARS: RA-5(CMS-1); HIPAA: 164.306(a)(2); HSPD 7: G(24)	Related Controls:

ASSESSMENT PROCEDURE: RA-5(CMS-1).1

Assessment Objective

Determine if:
(i) the organization defines the frequency of vulnerability scans within the information system;
(ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported; and
(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for vulnerability scanning); vulnerability scanning results; patch and vulnerability management records; other relevant documents or records to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE) naming convention.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE) naming convention.

System and Services Acquisition (SA) – *Management*

SA-1 – System and Services Acquisition Policy and Procedures (Low)

Control

Documented procedures shall be developed and implemented effectively to facilitate the implementation of the system and services acquisition security controls in all system and services acquisitions. Procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and services acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: SA-1; IRS-1075: 5.6.1.3#1.1-2; NIST 800-53/53A: SA-1; PISP: 4.15.1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and services acquisition policy and procedures;
(ii) the organization disseminates system and services acquisition policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and services acquisition policy and procedures; and
(iv) the organization updates system and services acquisition policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)

ASSESSMENT PROCEDURE: SA-1.2

Assessment Objective

Determine if:
(i) the system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and services acquisition policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and services acquisition procedures address all areas identified in the system and services acquisition policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)

SA-2 – Allocation of Resources (Low)

Control

As part of the capital planning and investment control processes, CMS or the external organization shall determine, document, and allocate the resources required to protect CMS information systems adequately. IS requirements shall be included in mission / business case planning, and a separate line item shall be established in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Guidance

The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST SP 800-65 provides guidance on integrating security into the capital planning and investment control process.

Applicability: All	**References:** ARS: SA-2; NIST 800-53/53A: SA-2; PISP: 4.15.2	**Related Controls:**

ASSESSMENT PROCEDURE: SA-2.1

Assessment Objective

Determine if:
(i) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system;
(ii) the organization determines security requirements for the information system in mission/business case planning;
(iii) the organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation; and
(iv) the organization's programming and budgeting process is consistent with NIST SP 800-65.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST SP 800-65; other relevant documents or records.

Interview: Organizational personnel with capital planning and investment responsibilities.(Optional)

SA-3 – Life Cycle Support (Low)

Control

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

Guidance

NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Applicability: All	**References:** ARS: SA-3; FISCAM: TAY-1.2.1, TCC-1.1.2; NIST 800-53/53A: SA-3; PISP: 4.15.3	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3.1

Assessment Objective

Determine if:

(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and

(ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation; other relevant documents or records.

Interview: Organizational personnel with information security and system life cycle development responsibilities.(Optional)

SA-3(CMS-1) – Enhancement (Low)

Control

Must comply with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

Applicability: All	**References:** ARS: SA-3(CMS-1); FISCAM: TCC-1.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3(CMS-1).1

Assessment Objective

Determine if:

(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and

(ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation; other relevant documents or records to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

Interview: Organizational personnel with information security and system life cycle development responsibilities to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

SA-3(FIS-1) – Enhancement (Low)

Control

Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.

Applicability: All	**References:** FISCAM: TCC-2.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: SA-3(FIS-1).1

Assessment Objective

Determine if the organizational detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.

Assessment Methods And Objects

Examine: Design system specifications.

Examine: Pertinent policies and procedures.

Interview: Programmer and programming supervisor.

SA-4 – Acquisitions (Low)

Control

Security requirements and/or security specifications shall be included, either explicitly or by reference, in all information system acquisition contracts based on an assessment of risk in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

Solicitation Documents
Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required:
4.15.4.1. Security capabilities;
4.15.4.2. Design and development processes;
4.15.4.3. Test and evaluation procedures; and
4.15.4.4. Documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats / vulnerabilities are identified and as new technologies are implemented

Use of Evaluated and Validated Products
For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources:

1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

Configuration Settings and Implementation Guidance
The information system required documentation shall include security configuration settings, including documentation explaining exceptions to the standard, and security implementation guidance.

Guidance

Solicitation Documents
The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST SP 800-36 provides guidance on the selection of information security products. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Information System Documentation
The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

Use of Tested, Evaluated, and Validated Products
NIST SP 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.

Configuration Settings and Implementation Guidance
The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on configuration settings for information technology products.

Applicability: All	**References:** ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4	**Related Controls:**

ASSESSMENT PROCEDURE: SA-4.1

Assessment Objective

Determine if:
(i) the organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards;
(ii) the organization's acquisition of commercial information technology products is consistent with NIST SP 800-23;
(iii) references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST SP 800-70; and

(iv) acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe:
- required security capabilities;
- required design and development processes;
- required test and evaluation procedures; and
- required documentation.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.(Optional)

SA-4(CMS-1) – Enhancement (Low)

Control

Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

Applicability: All	**References:** ARS: SA-4(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-4(CMS-1).1

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records to determine that all contracts and Statements of Work (SOW) that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities to determine that all contracts and SOW that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

SA-5 – Information System Documentation (Low)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

Guidance

Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Applicability: All	**References:** ARS: SA-5; FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1, TSD-3.1.2, TSD-3.1.3, TSP-3.3.2; IRS-1075: 5.6.1.3#1.3; NIST 800-53/53A: SA-5; PISP: 4.15.5	**Related Controls:**

ASSESSMENT PROCEDURE: SA-5.1

Assessment Objective

Determine if:
(i) the organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system;
(ii) the organization makes available information on configuring, installing, and operating the information system; and
(iii) the organization makes available information on effectively using the security features in the information system.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; other relevant documents or records.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.(Optional)

SA-5(CMS-1) – Enhancement (Low)		
Control Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.		
Applicability: All	**References:** ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(CMS-1).1		
Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance; and required personnel training to include administrators and users. **Interview:** Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance; and required personnel training to include administrators and users.		
SA-5(CMS-2) – Enhancement (Low)		
Control Maintain an updated list of related system operations and security documentation.		
Applicability: All	**References:** ARS: SA-5(CMS-2); FISCAM: TSD-1.1.6	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(CMS-2).1		
Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization maintains an updated list of related system's operations and security documentation. **Interview:** Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization maintains an updated list of related system's operations and security documentation.		
SA-5(CMS-3) – Enhancement (Low)		
Control Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.		
Applicability: All	**References:** ARS: SA-5(CMS-3); FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1	**Related Controls:**
ASSESSMENT PROCEDURE: SA-5(CMS-3).1		
Assessment Objective Determine if responsible parties within the organization periodically review system and services acquisition policy and procedures. **Assessment Methods And Objects** **Examine:** System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization updates documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation. **Interview:** Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine if the organization updates documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.		
SA-5(FIS-1) – Enhancement (Low)		
Control Goals are established by senior management on the availability of data processing and on-line services. Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.		

Applicability: All	References: FISCAM: TSC-2.4.6, TSC-2.4.9	Related Controls:

ASSESSMENT PROCEDURE: SA-5(FIS-1).1

Assessment Objective

Determine if the organizational goals are established by senior management on the availability of data processing and on-line services. Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation.

Interview: Senior management, data processing management, and user management.

SA-5(FIS-2) – Enhancement (Low)

Control

Records are maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.

Applicability: All	References: FISCAM: TSC-2.4.7, TSC-2.4.8	Related Controls:

ASSESSMENT PROCEDURE: SA-5(FIS-2).1

Assessment Objective

Determine if the organizational records are maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation.

Interview: Senior management, data processing management, and user management.

SA-6 – Software Usage Restrictions (Low)

Control

All software or shareware and associated documentation used on CMS information systems shall be deployed and maintained in accordance with appropriate license agreements and copyright laws. Software associated documentation protected by quantity licenses shall be managed through a tracking system to control copying and distribution. All other uses not specifically authorized by the license agreement shall be prohibited. The use of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Guidance

Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Applicability: All	References: ARS: SA-6; FISCAM: TCC-2.3.1; IRS-1075: 4.7.3#1.2; NIST 800-53/53A: SA-6; PISP: 4.15.6	Related Controls:

ASSESSMENT PROCEDURE: SA-6.1

Assessment Objective

Determine if:

(i) the organization complies with software usage restrictions; and

(ii) the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records.

Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.(Optional)

SA-6(FIS-1) – Enhancement (Low)

Control

Implementation orders, including effective date, are provided to all locations where they are maintained on file.

Applicability: All	References: FISCAM: TCC-2.3.2	Related Controls:

ASSESSMENT PROCEDURE: SA-6(FIS-1).1

Assessment Objective

Determine if the organization provides to all locations software implementation orders, including effective date, where the orders are maintained on file.

Assessment Methods And Objects

Examine: Implementation orders.

Examine: Pertinent policies and procedures.

Interview: Information system and security administrators.

SA-7 – User Installed Software (Low)

Control

All users shall be restricted from downloading or installing software, unless explicitly authorized in writing by the CIO or his/her designated representative. Users that have been granted such authorization may download and install only organization-approved software. The use of install-on-demand software shall be restricted.

Guidance

If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Applicability: All	References: ARS: SA-7; FISCAM: TCC-1.3.1; NIST 800-53/53A: SA-7; PISP: 4.15.7	Related Controls:

ASSESSMENT PROCEDURE: SA-7.1

Assessment Objective

Determine if:

(i) the organization enforces explicit rules governing the installation of software by users;

(ii) unauthorized software is present on the system; and

(iii) the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary action.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records.

Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.(Optional)

Test: Enforcement of rules for user installed software on the information system; information system for prohibited software.(Optional)

SA-7(CMS-1) – Enhancement (Low)

Control

If user installed software is authorized in writing by the CIO or his/her designated representative, ensure that business rules and technical controls enforce the documented authorizations and prohibitions.

Applicability: All	References: ARS: SA-7(CMS-1)	Related Controls:

ASSESSMENT PROCEDURE: SA-7(CMS-1).1

Assessment Objective

Determine if the organization enforces explicit rules governing the installation of software by users.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records to determine that policies exist that ensure business rules and technical controls enforce the documented authorizations and prohibitions.

Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine that policies exist that ensure business rules and technical controls enforce the documented authorizations and prohibitions.

SA-9 – External Information System Services (Low)

Control

All external information system services shall include specific provisions requiring the service provider to comply with CMS IS policies, standards, and guidelines; and shall be monitored for compliance. CMS shall define the remedies for any loss, disruption, or damage caused by the service provider's failure to comply. Service providers shall be prohibited from outsourcing any system function overseas, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representatives with concurrence from CMS' personnel security department.

Guidance

An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on the security considerations in the system development life cycle.

Applicability: All	**References:** ARS: SA-9; FISCAM: TAY-1.3.1; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4; NIST 800-53/53A: SA-9; PISP: 4.15.9	**Related Controls:** CA-3

ASSESSMENT PROCEDURE: SA-9.1

Assessment Objective

Determine if:

(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;

(ii) the organization monitors security control compliance;

(iii) the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions; and

(iv) the security controls employed by providers of external information system services are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.(Optional)

SA-9(CMS-1) – Enhancement (Low)

Control

If service providers are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas, ensure that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Applicability: All	**References:** ARS: SA-9(CMS-1); HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8)	**Related Controls:**

ASSESSMENT PROCEDURE: SA-9(CMS-1).1

Assessment Objective

Determine if the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

System and Communications Protection (SC) – *Technical*

SC-1 – System and Communications Protection Policy and Procedures (Low)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**References:** ARS: SC-1; FISCAM: TAC-3.2.E.1; IRS-1075: 5.6.3.4#1, 5.6.3.4#2; NIST 800-53/53A: SC-1; PISP: 4.16.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and communications protection policy and procedures;
(ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and
(iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and communications protection responsibilities.(Optional)

ASSESSMENT PROCEDURE: SC-1.2

Assessment Objective

Determine if:
(i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and communications protection responsibilities.(Optional)

SC-2 – Application Partitioning (Low)

Control

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Guidance

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Applicability: All	**References:** ARS: SC-2; NIST 800-53/53A: SC-2; PISP: 4.16.2	**Related Controls:**

ASSESSMENT PROCEDURE: SC-2.1

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Separation of user functionality from information system management functionality.(Optional)

SC-2(CMS-1) – Enhancement (Low)

Control

Implement DMZ architecture to separate internal network from public systems, and CMS servers from unnecessary public access, physically partitioning applications of varying sensitivity levels.

Applicability: All	**References:** ARS: SC-2(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-2(CMS-1).1

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Interview: Selected organizational personnel with network administration responsibilities to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

SC-5 – Denial of Service Protection (Low)

Control

Mechanisms shall be established to prevent, or limit the effects of well-known, detectable, and preventable denial-of-service attacks.

Guidance

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Applicability: All	**References:** ARS: SC-5; NIST 800-53/53A: SC-5; PISP: 4.16.5	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5.1

Assessment Objective

Determine if:

(i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and

(ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for protection against or limitation of the effects of denial of service attacks.(Optional)

SC-5(0) – Enhancement (Low)

Control

Protect the information system against the denial-of-service attacks defined on the following sites or within the following documents:

- SANS Organization www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and
- NIST CVE List http://checklists.nist.gov/home.cfm.

Applicability: All	**References:** ARS: SC-5(0); NIST 800-53/53A: SC-5; PISP: 4.16.5	**Related Controls:**

ASSESSMENT PROCEDURE: SC-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan (for list of organization-defined types of denial of service attacks to protect against or limit); information system configuration settings and associated documentation; other relevant documents or records.

SC-5(1) – Enhancement (Low)		
Control Restrict the ability of users to launch denial of service attacks against other information systems or networks.		
Applicability: All	**References:** ARS: SC-5(1); NIST 800-53/53A: SC-5(1)	**Related Controls:**
ASSESSMENT PROCEDURE: SC-5(1).1		
Assessment Objective Determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks. **Assessment Methods And Objects** **Examine:** System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].(Optional) **Test:** Information system for protection against or limitation of the effects of denial of service attacks].(Optional)		
SC-5(2) – Enhancement (Low)		
Control Maintain excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.		
Applicability: All	**References:** ARS: SC-5(2); NIST 800-53/53A: SC-5(2)	**Related Controls:**
ASSESSMENT PROCEDURE: SC-5(2).1		
Assessment Objective Determine if the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks. **Assessment Methods And Objects** **Examine:** System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].(Optional)		
SC-7 – Boundary Protection (Low)		
Control Automated boundary protection mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces. The operational failure of the boundary protection mechanisms shall not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing site shall provide the same levels of protection as those of the primary site.		
Guidance Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning. The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-77 provides guidance on virtual private networks.		
Applicability: All	**References:** ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	**Related Controls:** AC-4, CA-3, MP-4, RA-2
ASSESSMENT PROCEDURE: SC-7.1		
Assessment Objective Determine if: (i) the organization defines key internal boundaries of the information system; and (ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.		

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.(Optional)

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system.(Optional)

SC-7(5) – Enhancement (Low)

Control

Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.

Applicability: All	**References:** ARS: SC-7(5); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(5).1

Assessment Objective

Determine if the information system denies network traffic by default and allows network traffic by exception.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Interview: Selected organizational personnel with boundary protection responsibilities.(Optional)

SC-7(CMS-1) – Enhancement (Low)

Control

Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Applicability: All	**References:** ARS: SC-7(CMS-1)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(CMS-1).1

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

SC-7(CMS-2) – Enhancement (Low)

Control

Although not required, it is recommended that stateful inspection hardware and software is utilized.

Applicability: All	**References:** ARS: SC-7(CMS-2); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-7(CMS-2).1

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes stateful inspection / application firewall hardware and software.

SC-10 – Network Disconnect (Low)

Control

Technical controls shall be established and implemented effectively to ensure that network connections are properly terminated at the end of user sessions, or upon the occurrence of specified conditions (e.g., a period of inactivity).

Guidance

The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Applicability: All	**References:** ARS: SC-10; NIST 800-53/53A: SC-10; PISP: 4.16.10	**Related Controls:**

ASSESSMENT PROCEDURE: SC-10.1

Assessment Objective

Determine if:
(i) the organization defines the time period of inactivity before the information system terminates a network connection; and
(ii) the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.(Optional)
Test: Network disconnect capability within the information system.(Optional)

SC-10(0) – Enhancement (Low)

Control

Configure the information system to forcibly disconnect network connections at the end of a session, or after fifteen (15) minutes of inactivity, for mainframe sessions.

Applicability: All	**References:** ARS: SC-10(0); FISCAM: TAC-3.2.C.3; PISP: 4.16.10	**Related Controls:**

ASSESSMENT PROCEDURE: SC-10(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.

SC-13 – Use of Cryptography (Low)

Control

When cryptographic mechanisms are used, procedures shall be developed, documented, and implemented effectively to ensure they comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. All such mechanisms shall be FIPS 140-2 (as amended and revised) compliant and NIST validated.

Guidance

The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	**References:** ARS: SC-13; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2, 5.6.3.4#4.2-3; NIST 800-53/53A: SC-13; PISP: 4.16.13	**Related Controls:** AC-17(CMS-1), AC-19(CMS-1), AC-3, AC-3(CMS-1), MP-4(PII-1), SC-12(CMS-1), SC-8(CMS-1), SC-9(1)

ASSESSMENT PROCEDURE: SC-13.1

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

SC-14 – Public Access Protections (Low)

Control

Technical controls shall be developed, documented, and implemented effectively to protect the integrity of the publicly accessible CMS information and applications.

Guidance

CMS refers to the National Institute of Standards and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix A provides a summary for remote access controls.

Applicability: All	**References:** ARS: SC-14; NIST 800-53/53A: SC-14; PISP: 4.16.14	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14.1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing access controls and boundary protection for publicly available information and applications within the information system.(Optional)

SC-14(CMS-1) – Enhancement (Low)

Control

Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

Applicability: All	**References:** ARS: SC-14(CMS-1); FISCAM: TAC-3.2.E.1	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14(CMS-1).1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

Interview: Organizational personnel to determine if network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.

SC-14(CMS-2) – Enhancement (Low)

Control

If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.

Applicability: All	**References:** ARS: SC-14(CMS-2)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-14(CMS-2).1

Assessment Objective

Determine if the information system protects the integrity and availability of publicly available information and applications.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.

Interview: MA owners for each public-facing MA to determine if e-authentication is required and implemented in conjunction with or related to public access protections; refer to ARS Appendix A for e-Authentication Standards.

SC-CMS-1 – Desktop Modems (Low)

Control

Users are prohibited from installing desktop modems.

Guidance

Desktop Modems allow backdoors into the network putting the CMS data and network at very high risk.

Applicability: All	**References:** ARS: SC-CMS-1; PISP: 4.16.24	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-1.1

Assessment Objective

Determine if the organization has implement a policy which assists in prohibiting the installation of unauthorized desktop modems.

Assessment Methods And Objects

Examine: Organizational policy does not allow unauthorized desktop modems.

SC-CMS-2 – Identify and Detect Unauthorized Modems (Low)

Control

Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized modems.

Guidance

It is good practice that management approve any automated tool or utility for checking for unauthorized modems.

Applicability: All	**References:** ARS: SC-CMS-2; PISP: 4.16.25	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-2.1

Assessment Objective

Determine if the organization has an approved automated system to test for unauthorized modems.

Assessment Methods And Objects

Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

SC-CMS-2(CMS-0) – Enhancement (Low)

Control

Examine a sample of network systems using an automated method no less than quarterly to determine if unauthorized modems are present.

Applicability: All	**References:** ARS: SC-CMS-2(CMS-0)	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

SC-CMS-3 – Secondary Authentication and Encryption (Low)

Control

Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network.

Guidance

A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP.

Applicability: All	**References:** ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-3.1

Assessment Objective

Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit.

Assessment Methods And Objects

Examine: In-transit technical controls implement and documents for sensitive information outside the secure network.

SC-CMS-3(CMS-0) – Enhancement (Low)		
Control No specific requirements but recommend enabling application security mechanisms, such as Transport Layer Security (TLS), and utilizing minimum encryption and password authentication.		
Applicability: All	**References:** ARS: SC-CMS-3(CMS-0)	**Related Controls:**
ASSESSMENT PROCEDURE: SC-CMS-3(CMS-0).1		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** **Examine:** Documentation to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization utilizes CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric). **Interview:** Organizational personnel to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization utilizes CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).		
SC-CMS-3(CMS-1) – Enhancement (Low)		
Control If e-authentication is required and implemented, refer to ARS Appendix A for e-Authentication Standards controls and procedures.		
Applicability: All	**References:** ARS: SC-CMS-3(CMS-1)	**Related Controls:**
ASSESSMENT PROCEDURE: SC-CMS-3(CMS-1).1		
Assessment Objective Determine if the organization that uses e-authentication is required to refer to ARS Appendix A for e-Authentication Standards controls and procedures. **Assessment Methods And Objects** **Examine:** Network documentation to determine which recommends enabling application security mechanisms, such as TLS, and utilizing minimum encryption and password authentication although, no specific requirements are mandatory. **Interview:** Organizational personnel to determine if enabling application security mechanisms is recommended, such as TLS, and utilizing minimum encryption and password authentication although, no specific requirements are mandatory.		
SC-CMS-5 – Persistent Cookies (Low)		
Control The use of persistent cookies on a CMS web site is prohibited unless explicitly approved in writing by the DHHS Secretary.		
Guidance Requests to DHHS should be via CMS.		
Applicability: All	**References:** ARS: SC-CMS-5; PISP: 4.16.28	**Related Controls:**
ASSESSMENT PROCEDURE: SC-CMS-5.1		
Assessment Objective Determine if the organization does not use a persistent cookie configuration on a CMS web site to remember subsequent visits unless approved in writing by the DHHS Secretary. **Assessment Methods And Objects** **Examine:** CMS web site baseline and change management documentation for configurations using persistent cookies. **Interview:** Web site administrators to determine if the CMS web site has persistent cookies enable in the baseline configuration or have written approval to enable persistent cookies from the DHHS Secretary.		
SC-CMS-6 – Network Interconnection (Low)		
Control Controls shall be developed, documented, and implemented effectively to ensure that only properly authorized network interconnections external to the system boundaries are established.		
Guidance A good place to obtain technical controls for securing interconnections external to the system boundaries is the NIST SP.		
Applicability: All	**References:** ARS: SC-CMS-6; PISP: 4.16.29	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-6.1

Assessment Objective

Determine if the organization effectively documents and implements authorized network interconnections external to the system boundaries.

Assessment Methods And Objects

Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards for all external interconnections.

SC-CMS-6(CMS-0) – Enhancement (Low)

Control

Ensure remote location(s) (e.g., users and sites using a network interconnection external to the system boundaries) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

Applicability: All	**References:** ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2	**Related Controls:**

ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

Interview: Personnel to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.

System and Information Integrity (SI) – *Operational*

SI-1 – System and Information Integrity Policy and Procedures (Low)

Control

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems, software, and information. The procedures and automated mechanisms shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. It is good practice to have an automated system which is host based to automatically detect, block/filter and alert supervisors or managers that possible unauthorized changes to software and the information system have occurred.

Applicability: All	**References:** ARS: SI-1; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-1; PISP: 4.17.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and information integrity policy and procedures;
(ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review system and information integrity policy and procedures; and
(iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and information integrity responsibilities.(Optional)

ASSESSMENT PROCEDURE: SI-1.2

Assessment Objective

Determine if:
(i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
(iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and information integrity responsibilities.(Optional)

SI-2 – Flaw Remediation (Low)

Control

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. The flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

Guidance

The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. It is a good practice to test the changes in a laboratory environment on like systems prior to approving and implementing the updates and changes. NIST SP 800-40, provides guidance on security patch installation and patch management.

Applicability: All	**References:** ARS: SI-2; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2; PISP: 4.17.2	**Related Controls:** CA-2, CA-4, CA-7, CM-3, IR-4, SI-11

ASSESSMENT PROCEDURE: SI-2.1

Assessment Objective

Determine if:
(i) the organization identifies, reports, and corrects information system flaws;
(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;
(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;
(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and
(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.(Optional)

SI-2(0) – Enhancement (Low)

Control

Correct identified information system flaws on production equipment within one (1) month.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and
(b) Manage the flaw remediation process centrally.

Applicability: All	**References:** ARS: SI-2(0); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2; PISP: 4.17.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.(Optional)

SI-2(1) – Enhancement (Low)

Control

Updates are installed automatically.

Applicability: All	**References:** ARS: SI-2(1); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-2(1).1

Assessment Objective

Determine if the organization centrally manages the flaw remediation process and installs updates automatically.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records.(Optional)

Test: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates.(Optional)

SI-2(2) – Enhancement (Low)

Control

Employ automated mechanisms periodically and upon demand to determine the state of information system components with regard to flaw remediation.

Applicability: All	**References:** ARS: SI-2(2); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-2(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing information system flaw remediation update status.(Optional)

SI-3 – Malicious Code Protection (Low)

Control

Automated malicious code protection mechanisms that include a capability of automatic updates shall be in place and supporting procedures shall be developed, documented, and implemented effectively to identify and isolate suspected malicious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical information system entry points, and at each workstation, server, or mobile computing device on the network to detect and eradicate malicious code transported by email, email attachments, removable media or other methods. Business owners shall use antiviral software products from multiple vendors, if possible, and update virus protection mechanisms whenever new releases are available.

Guidance

The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST SP 800-83 provides guidance on implementing malicious code protection.

Applicability: All	**References:** ARS: SI-3; FISCAM: TCC-1.3.2; IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3.1

Assessment Objective

Determine if:

(i) the information system implements malicious code protection;

(ii) the organization employs malicious code protection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;

(iii) the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities;

(iv) the organization updates malicious code protection mechanisms whenever new releases are available; and

(v) the malicious code protection mechanisms are appropriately updated to include the latest malicious code definitions, configured to perform periodic scans of the information system as well as real-time scans of files from external sources as the files are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(0) – Enhancement (Low)

Control

Implement malicious code protection at information system entry points, including firewalls, email servers, remote access servers, workstations, servers, and mobile computing devices by employing automated mechanisms to detect and eradicate malicious code transported by email, email attachments, and removable media.

Applicability: All	**References:** ARS: SI-3(0); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection

updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(1) – Enhancement (Low)

Control

Manage and update malicious code protection software centrally with automatic updates for the latest malicious code definitions whenever new releases are available.

Applicability: All	**References:** ARS: SI-3(1); IRS-1075: 5.6.2.5#1.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(1).1

Assessment Objective

Determine if the organization centrally manages malicious code protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SI-3(2) – Enhancement (Low)

Control

Employ automated mechanisms to update malicious code protection.

Applicability: All	**References:** ARS: SI-3(2); IRS-1075: 5.6.2.5#1.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(2).1

Assessment Objective

Determine if the organization automatically updates malicious code protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Automatic update capability for malicious code protection.(Optional)

SI-3(CMS-1) – Enhancement (Low)

Control

Enable real-time file scanning. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and once a week.

Applicability: All	**References:** ARS: SI-3(CMS-1); IRS-1075: 5.6.2.5#1.3	**Related Controls:**

ASSESSMENT PROCEDURE: SI-3(CMS-1).1

Assessment Objective

Determine if:

(i) real-time file scanning is enabled;

(ii) real-time desktop malicious code scanning is enabled and monitored; and

(iii) software is configured to perform critical system file scans during system boot and once a week.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records to determine real-time file scanning is enabled. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and once a week.

Interview: Personnel with system and information integrity responsibilities to determine real-time file scanning is enabled, desktop malicious code scanning software is installed, real-time protection, and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and once a week.

SI-4 – Information System Monitoring Tools and Techniques (Low)

Control

Effective monitoring tools and techniques providing real-time identification of unauthorized use, misuse, and abuse of the information system shall be implemented.

Guidance

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices

are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST SP 800-61 provides guidance on detecting attacks through various types of security technologies. NIST SP 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST SP 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST SP 800-94 provides guidance on intrusion detection and prevention.

Applicability: All	**References:** ARS: SI-4; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4; PISP: 4.17.4	**Related Controls:** AC-8, AU-4, CM-6

ASSESSMENT PROCEDURE: SI-4.1

Assessment Objective

Determine if the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SI-4(1) – Enhancement (Low)

Control

Connect individual IDS devices to a common IDS management network using common protocols.

Applicability: All	**References:** ARS: SI-4(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(1)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(1).1

Assessment Objective

Determine if the organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.(Optional)

Test: Information system-wide intrusion detection capability.(Optional)

SI-4(5) – Enhancement (Low)

Control

Real-time alerts are provided when indications of the following types of compromise, or potential compromise, occur:
(a) Presence of malicious code,
(b) Unauthorized export of information,
(c) Signaling to an external information system, or
(d) Potential intrusions.

Applicability: All	**References:** ARS: SI-4(5)	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(5).1

Assessment Objective

Determine if:
(i) the organization identifies indications of compromise or potential compromise to the security of the information system; and
(ii) the information system provides a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Information system monitoring real-time alert capability.(Optional)

SI-4(CMS-1) – Enhancement (Low)

Control

Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.

Applicability: All	**References:** ARS: SI-4(CMS-1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4	**Related Controls:**

ASSESSMENT PROCEDURE: SI-4(CMS-1).1

Assessment Objective

Determine if:
(i) IDS devices are installed at network perimeter points; and
(ii) host-based IDS sensors are installed on critical servers.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

Interview: Personnel with system and information integrity responsibilities to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

SI-5 – Security Alerts and Advisories (Low)

Control

Procedures shall be developed, documented, and implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis, and for issuing IS alerts and advisories to appropriate personnel. Upon receipt of such alerts and advisories, personnel shall take appropriate response actions. The types of actions to be taken in response to security alerts / advisories shall be documented.

Guidance

The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST SP 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Applicability: All	**References:** ARS: SI-5; NIST 800-53/53A: SI-5; PISP: 4.17.5	**Related Controls:**

ASSESSMENT PROCEDURE: SI-5.1

Assessment Objective

Determine if:
(i) the organization receives information system security alerts/advisories on a regular basis;
(ii) the organization issues security alerts/advisories to appropriate organizational personnel; and
(iii) the organization takes appropriate actions in response to security alerts/advisories.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; NIST SP 800-40; records of security alerts and advisories; other relevant documents or records.

Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system.(Optional)

SI-7 – Software and Information Integrity (Low)

Control

Automated mechanisms for software and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to software. Good software engineering practices consistent with CMS IS policy and procedures shall be employed with regard to commercial-off-the-shelf (COTS) integrity mechanisms, and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications.

Guidance

The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Applicability: All	**References:** ARS: SI-7; FISCAM: TAN-3.1.2, TAN-3.2.1, TAN-3.2.2, TAY-2.1.4, TAY-2.2.2, TCP-2.1.2, TCP-2.1.3, TCP-2.1.4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7; PISP: 4.17.7	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7.1

Assessment Objective

Determine if:
(i) the information system detects and protects against unauthorized changes to software and information; and

(ii) the organization employs effective integrity verification tools in accordance with good software engineering practices.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records.(Optional)

Test: Software integrity protection and verification capability.(Optional)

SI-7(FIS-1) – Enhancement (Low)

Control

A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing. Live data are not used in testing of program changes except to build test data files.

Applicability: All	**References:** FISCAM: TCC-2.1.6, TCC-2.1.7	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-1).1

Assessment Objective

Determine if:

(i) the organization provides a comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.

(ii) the organizational validation does not use live data in testing of program changes except to build test data files.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Test transactions and data.

Interview: Programmers, auditors, and quality assurance personnel.

SI-7(FIS-2) – Enhancement (Low)

Control

User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.

Applicability: All	**References:** FISCAM: TCP-1.1.1	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-2).1

Assessment Objective

Determine if the organizational user-prepared record count and control totals documents help determine the completeness of data entry and processing.

Assessment Methods And Objects

Examine: Activity for developing record counts and control totals.

Examine: Application documentation.

Examine: Pertinent policies and procedures.

Interview: User management and personnel.

SI-7(FIS-3) – Enhancement (Low)

Control

For on-line or real-time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing.

Applicability: All	**References:** FISCAM: TCP-1.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-7(FIS-3).1

Assessment Objective

Determine if the organizational on-line or real-time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing.

Assessment Methods And Objects

Examine: Application documentation.

Examine: Pertinent policies and procedures.

Examine: Supporting documentation generated by system.

Interview: Application programmer, if available.

Interview: User management and personnel.

SI-7(FIS-4) – Enhancement (Low)		
Control Record counts and control totals are established over and entered with transaction data, and reconciled to determine the completeness of data entry.		
Applicability: All	**References:** FISCAM: TCP-2.1.1	**Related Controls:**
ASSESSMENT PROCEDURE: SI-7(FIS-4).1		
Assessment Objective Determine if the organizational record counts and control totals are established over and entered with transaction data, and reconciled to determine the completeness of data entry. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Pertinent policies and procedures. **Examine:** Reconciliation activities. **Interview:** Data control personnel. **Interview:** User management and personnel.		
SI-7(FIS-5) – Enhancement (Low)		
Control Reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated.		
Applicability: All	**References:** FISCAM: TCP-2.2.1	**Related Controls:**
ASSESSMENT PROCEDURE: SI-7(FIS-5).1		
Assessment Objective Determine if the organizational reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Pertinent policies and procedures. **Examine:** Reconciliation activities. **Interview:** Data control personnel. **Interview:** User management and personnel.		
SI-8 – Spam Protection (Low)		
Control Automated mechanisms for spam protection shall be in place at critical information system entry points, workstations, servers, and mobile computing devices on the network. Supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect spam.		
Guidance The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST SP 800-45 provides guidance on electronic mail security.		
Applicability: All	**References:** ARS: SI-8; HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8; PISP: 4.17.8	**Related Controls:**
ASSESSMENT PROCEDURE: SI-8.1		
Assessment Objective Determine if: (i) the information system implements spam protection; (ii) the organization employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network; (iii) the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail; and (iv) the organization updates spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures. **Assessment Methods And Objects** **Examine:** System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.(Optional) **Test:** Spam detection and handling capability.(Optional)		

SI-12 – Information Output Handling and Retention (Low)

Control

Output from information systems shall be handled and retained in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, operational requirements, and the information sensitivity level.

Guidance

A good place to obtain procedures for handling sensitive output information is the NIST SP.

Applicability: All	**References:** ARS: SI-12; FISCAM: TAY-4.1.6; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2; NIST 800-53/53A: SI-12; PISP: 4.17.12	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12.1

Assessment Objective

Determine if:

(i) the organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and

(ii) the organization handles output from the information system in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records.(Optional)

Interview: Organizational personnel with information output handling and retention responsibilities.(Optional)

SI-12(CMS-1) – Enhancement (Low)

Control

Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements.

Applicability: All	**References:** ARS: SI-12(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12(CMS-1).1

Assessment Objective

Determine if the organization retains output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable NARA requirements.

Assessment Methods And Objects

Examine: At a minimum, documentation for record retention audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements are met.

SI-12(FIS-1) – Enhancement (Low)

Control

Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design by a data processing control group, or some alternative. A data processing control group: (1) has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; (2) reviews output products for general acceptability; and (3) reconciles control information to determine completeness of processing.

Applicability: All	**References:** FISCAM: TAY-4.1.1, TAY-4.1.2	**Related Controls:**

ASSESSMENT PROCEDURE: SI-12(FIS-1).1

Assessment Objective

Determine if the organization assigns responsibility for seeing that all outputs are produced and distributed according to system requirements and design by a data processing control group, or some alternative. A data processing control group: (1) has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; (2) reviews output products for general acceptability; and (3) reconciles control information to determine completeness of processing.

Assessment Methods And Objects

Examine: Output production and distribution.

Examine: Pertinent policies and procedures.

Interview: Information system and user management.

SI-12(FIS-2) – Enhancement (Low)		
Control Printed reports contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message.		
Applicability: All	**References:** FISCAM: TAY-4.1.3	**Related Controls:**
ASSESSMENT PROCEDURE: SI-12(FIS-2).1		
Assessment Objective Determine if the organizational information system printed reports contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Printed reports. **Interview:** User personnel and application programmer, if available.		
SI-12(FIS-3) – Enhancement (Low)		
Control Each output produced, whether printed or transmitted to a user's terminal device, is logged, manually if not automatically, including the recipient(s) who receive the output.		
Applicability: All	**References:** FISCAM: TAY-4.1.4, TAY-4.1.5	**Related Controls:**
ASSESSMENT PROCEDURE: SI-12(FIS-3).1		
Assessment Objective Determine if the organizational information system's output produced, whether printed or transmitted to a user's terminal device, is logged, manually if not automatically, including the recipient(s) who receive the output. **Assessment Methods And Objects** **Examine:** Application documentation. **Examine:** Output logs. **Interview:** Information system and user personnel.		
SI-12(FIS-4) – Enhancement (Low)		
Control In the user department, outputs transmitted are summarized daily and printed for each terminal device, and reviewed by supervisors. A control log of output product errors is maintained, including the corrective actions take.		
Applicability: All	**References:** FISCAM: TAY-4.1.7, TAY-4.1.8	**Related Controls:**
ASSESSMENT PROCEDURE: SI-12(FIS-4).1		
Assessment Objective Determine if the organizational information system's user department, outputs transmitted are summarized daily and printed for each terminal device, and reviewed by supervisors. A control log of output product errors is maintained, including the corrective actions take. **Assessment Methods And Objects** **Examine:** Pertinent policies and procedures. **Examine:** Supporting documentation (e.g., printed daily summaries with supervisory initials or signatures). **Examine:** This activity. **Interview:** User supervisory personal.		
SI-12(FIS-5) – Enhancement (Low)		
Control Users review output reports for data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction reports, (3) master record change reports, (4) exception reports, and (5) control totals balance reports. Output from reruns is subjected to the same quality review as the original output.		
Applicability: All	**References:** FISCAM: TAY-4.1.9, TAY-4.2.1	**Related Controls:**
ASSESSMENT PROCEDURE: SI-12(FIS-5).1		
Assessment Objective Determine if the organizational users review output reports for data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction reports, (3) master record change		

reports, (4) exception reports, and (5) control totals balance reports. Output from reruns is subjected to the same quality review as the original output.

Assessment Methods And Objects

Examine: Activity to review output reports.
Examine: Output reports.
Examine: Pertinent policies and procedures.
Interview: User management and personnel.

Appendix B:
Medicare Information Technology (IT) Systems Contingency Planning

Table of Contents

(Rev. 9, 06-20-08)

1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS business partners are required by CMS CSR 5.2 to develop and maintain a contingency plan. This plan is to provide information to aid the business partner in planning for and responding to an emergency or system disruption, and to recover from that emergency or disruption.

Section 3.4 of this document requires that all CMS Medicare business partners prepare, review, and test their Medicare IT systems contingency plans. All General Support Systems (GSS) and Major Applications (MA) that support critical Medicare operations *shall* be covered by a Medicare IT Systems Contingency Plan (CP).

This document presents the direction for accomplishing Medicare IT systems contingency planning. It is to be used by the CMS Medicare business partner management, IT systems management and staff, and system security persons charged with preparing for continuing the operation of Medicare systems and developing an IT systems contingency plan, or updating an existing plan.

The business partner information security risk assessment may be used as a checkpoint to determine if appropriate contingencies have been addressed in the contingency plan.

To ensure the contingency plan is workable, it *shall* be thoroughly and periodically tested.

The simplified diagram in Figure B-1 illustrates the IT systems contingency planning process.

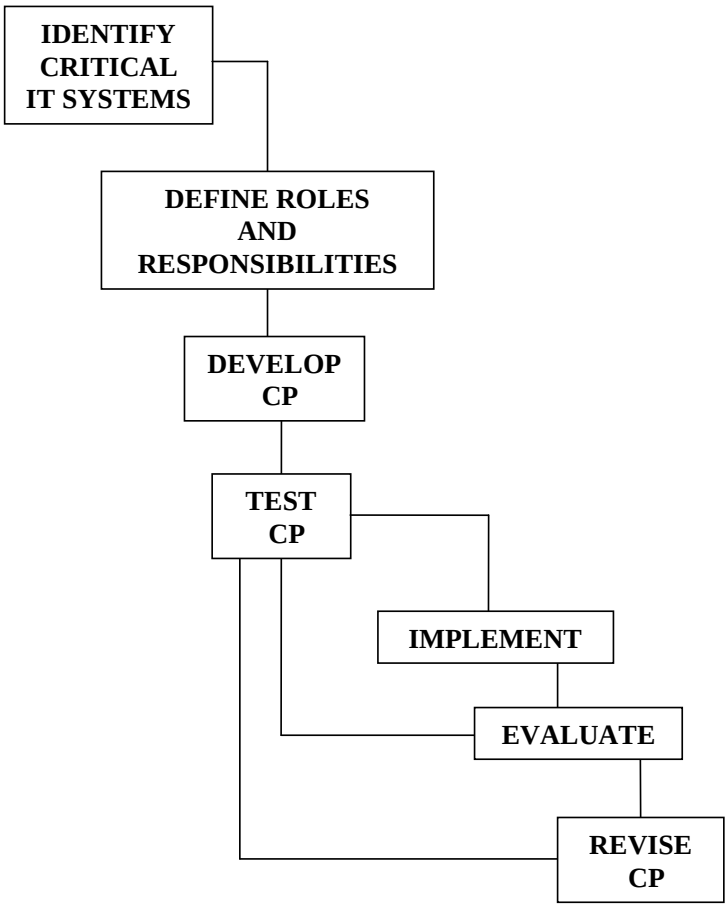

Figure B-1 – IT Systems Contingency Planning Process

3 Definition of an Acceptable Contingency Plan

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A contingency plan is a document that describes how to plan for and deal with an emergency or system disruption. These situations could be caused by a power outage, hardware failure, fire, or terrorist activity. A contingency plan is developed and maintained to ensure quick, appropriate, effective, and efficient response in those situations for which a foreseen risk cannot be mitigated or avoided.

Protecting lives is the paramount task while executing a contingency plan.

Before developing an IT systems contingency plan, it is advisable to have or create a contingency policy. The contingency plan *shall* be driven by a contingency policy. The contingency policy is a high level statement relative to what the management wants to do to address a contingency and to recover from the emergency or system disruption.

The IT systems contingency plan *shall* be developed under the guidance of IT management and systems security persons and all organizational components *shall* be

actively involved in providing information for developing the plan, for making plan related decisions, and for providing support to plan testing.

It can be a very subjective argument relative to what constitutes an acceptable contingency plan. In this document, the description of an acceptable contingency plan is based on the results of the research, analysis and review of various documents from Government and industry, and the review of existing business partner contingency plans and test reports.

The following summary statements define what constitutes an acceptable contingency plan. This is not an all-inclusive list and the topics are not in any order of importance or priority.

1. Considers the protection of human life as the paramount guiding principle, and then aims at the backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high-quality service.

2. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.

3. Considers risk assessment results.

4. Addresses possible and probable emergencies or system disruptions.

5. Can be sufficiently tested on an established regular basis at reasonable cost.

6. Contains information that is needed and useful during an emergency or system disruption.

7. Can, when implemented, produce a response and recovery, such that critical business functions are continued.

8. Specifies the persons necessary to implement the plan, and clearly defines their responsibilities.

9. Clearly defines the resources necessary to implement the plan.

10. Reflects what can be done – is not a wish list.
11. Assumes people *shall* use sound judgment, but will need clearly stated guidance, since they will be functioning in a non-normal environment, under possibly severe pressure.

12. Addresses backup and alternate sites.

13. Addresses the use of manual operations, where appropriate and necessary.

14. Contains definitive “Call Lists” to use for contacting the appropriate persons in the proper sequence. This list would include vendor points of contact.

An acceptable contingency plan should be straight to the point. It should not contain any more information than is necessary to plan for and implement contingency actions. The users should not get bogged down in detail as they read the plan to determine what to do, when to do it, what is needed to do it, and who should do it. The contingency plan should serve as a “user’s manual” and be easy to understand and use.

Because a contingency plan is designed to be used in a stressful situation, it *shall* be written with that as a foremost thought in mind. The prime objective is to maximize the continuity of critical operations.

Reviewing a contingency plan and testing it will help determine whether it remains an acceptable plan. The review and testing *shall* not focus solely on content, but *shall* also focus on ease of use.

A complete set of contingency plans for an organization may be made up of several smaller contingency plans, one for each business function (e.g. claims processing) or for a single data center, for example. This breakdown into manageable parts helps to keep a plan easy to use.

Careful thought should be given to the organization of the contingency plan. The organization should be logical in terms of what will the user want to know or do first. If the first thing that should happen in an emergency is that a call list *shall* be used to notify persons, then that call list, or a pointer to it, should be placed very near the front of the contingency plan. Not every informational item to be utilized during a contingency event will be in the contingency plan document. For example, the plan may point to an attachment or to a separate procedures manual. In this regard, a contingency plan should contain a very understandable and useful table of contents, so that a user can quickly find the information being sought.

Contingency planning can provide a cost-effective way to ensure that critical IT capabilities can be recovered quickly after an emergency. IT systems contingency planning *shall* embrace a coordinated contingency policy of what will be done to fully recover and reconstitute all operations.

4.1 Contingency Planning

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Contingency planning is preparing for actions in the event of an emergency situation, and giving some thought and planning to what your organization will do to respond and recover. The IT systems contingency planning process *shall* address all the actions and resources needed to ensure continuity of operation of critical Medicare IT systems and the means of implementing the needed resources. IT management and staff *shall* be

trained to handle emergency or system disruption situations in data centers and other areas where data processing systems are located. Contingency planning includes such training.

It is advisable to establish a Medicare IT systems contingency planning team. This team would be responsible for defining critical Medicare IT systems, including applications software, data, processing and communications capabilities, and other supporting resources. These would be the key people in the implementation of the plan.

4.2 Coordination with Other Business Partners

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

If a business partner's data center or other data processing environment is linked to other business partners for the transmission of Medicare data, then the contingency planning *shall* include those links relative to receiving input, exchanging files, and distributing output. If alternate/backup IT systems capabilities are to be utilized, then their functions and data transmission links *shall* be considered in the planning.

Coordination with other business partners is essential to completing the IT systems contingency planning process.

5 Medicare IT Systems Contingency Plan

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The following format may be used in developing an IT system contingency plan. While this format is not required, all of its elements *shall* be included in the Contingency Plan.

1. Introduction
   - Background
   - Purpose/Objective
   - Management commitment statement
   - Scope
     - Organizations
     - Systems
     - Boundaries
   - IT capabilities and resources
   - CP policy
     - Priorities
     - Continuous operation
     - Recovery after short interruption
   - Minimum recovery times

2. Assumptions

3. Authority/References

4. Definition of what the CP addresses
    - Organizations
    - Systems
    - Boundaries

5. Three phases defined
    - Respond
    - Recover
    - Restore/reconstitute

6. Roles/Responsibilities defined

7. Definition of critical functions

8. Alternate capabilities and backup

9. Definition of required resources to respond and recover

10. Training
    - CP *shall* address Who – When – How

11. Testing the CP
    - Philosophy
    - Plans
    - Boundaries
    - Live vs. Walkthrough
    - Reports
    - Responsibilities

12. CP maintenance/updating
    - Schedule

13. Relationships/Interfaces
    - Outside (vendors, providers, banks, utilities, services, CMS)
    - Internal
    - Dependencies

14. Attachments
    - Actions for each phase
    - Procedures
    - Call trees
    - Vendor contact list
    - Hardware inventory
    - Software inventory

- System descriptions
- Alternate/Backup site information
- Assets/Resources
- Risk Assessment Summary (refer to System Security Plans)
- Agreements/Memos of Understanding
- Manual Operations
- Supplies/Materials/Equipment
- Floor plans
- Maps

The contingency plan *shall* provide for off-site storage:

- Backup software
- Data
- Appropriate documents (emergency telephone lists, memos of understanding, etc.)
- Copies of the contingency plan
- Administrative supplies (forms, blank check stock, etc.)

6 Testing

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS requires testing of the contingency plan annually under conditions that simulate an emergency or a disaster. *A contingency plan shall also be tested after a substantive system change that necessitates a revision to the contingency plan.*

CMS requires that the critical IT systems *shall* be tested annually and the contingency plan updated to accommodate any changes, including updated versions of software or critical data. Critical systems are those whose failure to function, for even a short time, could have a severe impact, or have a high potential for fraud, waste, or abuse.

6.1 Claims Processing Data Centers

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Many of the contractors with which CMS has direct contracts do not have their own data centers. They usually contract this service out. If a business partner does not have its own data center, then it is the responsibility of the business partner to inform the subcontractor that operates the data center that they *shall* have a contingency plan.

6.3 Test Types

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Contingency plan test guidance suggests *four (4)* types of testing:

- Walkthrough

- Simulation/modeling
- *Tabletop Test*
- Live

These are defined below:

- **Walkthrough**: A walkthrough test is accomplished by going through a set of steps to accomplish a particular task or action initiated because of a contingency event. The precursor to a walkthrough test is that the steps are documented so that they can be logically followed. A "test team" might sit around a table and talk through each step and then walk through" the various steps, and then discuss expected outcomes and further actions to be taken. They may use a checklist to ensure that all features of a step are addressed or that all resources necessary to accomplish the task or action are considered. A walkthrough test does not involve accomplishing the actions being tested in real time or using the live environment. A walkthrough test could be accomplished by using a group of test people to act out what might happen if a real contingency event occurred. They might go to the alternate site, but they would not actually start all hardware, software, and communication operations in order to assume the function of the primary site.

- **Simulation/Modeling**: Modeling involves creating a computer model of the process to be tested. This allows easy testing of many variables without physically having to make changes. For example, you can vary the number of servers that go down during a disaster or the number of people that can get to an alternate site following a disaster.

  Simulation involves taking physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team does the same at the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.

- ***Tabletop Test***: *For those applications that are both hosted at CMS and not participating in a broader recovery test to a CMS-approved recovery site during their annual test cycle, a tabletop test is required. A tabletop test is discussion-based only, and does not involve deploying equipment or other resources. The discussion during the test can be based on a single scenario or multiple scenarios. By simulating an emergency in an informal, stress-free environment, this test method allows for the free exchange of ideas and provides participants an opportunity to practice the steps to be followed in an actual event and to identify areas in the contingency plan for enhancement..*

  A successful tabletop test steps participants through real-life scenarios; captures its results in a formal report; and incorporates the "lessons learned" into subsequent versions of the contingency plan and the tabletop test plan. Refer to

CMS Contingency Planning Tabletop Test Procedures, for step-by-step instructions for conduction a tabletop test.

- **Live**: This is the most complete and expensive test to accomplish. It involves completing the physical steps that would actually be taken if an emergency occurred. People and materials would be moved to an alternate site for the test, and servers would actually be shut down to reduce capability. Power would be shut off, and live conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications, and people at the alternate site would be set into action and begin functioning as the primary site to support operations.

End-to-end refers to the scope of the testing (partial testing is less than end-to-end). When conducting end-to-end testing, items to consider include:

- End-to-end testing can be completed as part of walkthrough or live test.
- Not testing end-to-end means that some links, processes, or subsystems are missed.
- What is the risk in not conducting end-to-end testing?
- Live end-to-end testing can be very expensive!

Considering risks and cost, management *shall* make a decision as to what type and scope of testing is appropriate.

6.3.1 Live vs. Walkthrough

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

- High-level testing can take the form of a walkthrough test.
- A walkthrough can be part of the overall testing process, but not the whole process.
- Lower-level testing can include a walkthrough, if live testing is not an option.
  - Live testing *shall* be the first choice.
  - Fall back to a simulation/model if live testing is not an option. Cost, time, and interruption of normal operations are major considerations in doing a live test.
  - A walkthrough test should be the last resort.
- Ask what a walkthrough test would miss.

- Consider the ramifications of missing that part of the test.

- Remember that there is risk in not doing a live test—can the risk be accepted?
  - Consider the criticality of functions, processes, and systems.
    If critical to continuing essential business operations, then these are strong candidates for live testing.

- Testing interfaces.
  It is important to test the critical interfaces with internal and external systems. It is difficult to test interfaces using a "walkthrough" method. Simulation or "live" testing is preferred.

- Cost and complexity.
  The decision as to how to test critical functions, processes, and systems must result from careful consideration of complexity and cost. A complete "live" test of all elements of an operation may prove to be extremely costly, in terms of both dollars and time. If that cost out weighs the "cost" of the risk of not doing live testing, then "live" testing should probably be ruled out.

6.3.2 End-to-End

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This kind of testing aims to ensure that all software and hardware components associated with a function, process, or system are tested from the front end through to the back end (input through process through output). As with live testing, end-to-end testing can be expensive.

- End-to-end testing *shall* only be considered for critical functions, processes, or systems.

- Why is end-to-end testing needed?
  It provides the best assurance that there are no problems.

- Would a partial test be meaningful?
  If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical ones need be considered for end-to-end testing.

- Examples of types of end-to-end tests:
  - Claims receipt through to check generation
  - Query of a database through to the response
  - MSP check request through to check issue and back to MSP

- Evaluate complexity and cost.
  The decision on how to test critical functions, processes, and systems *shall* carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and

time. If that cost out weighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.

- Consider the criticality of functions, processes, and systems.
  Look at the criticality of functions, processes, and systems. If these are critical to continuing essential business operations, then these are strong candidates for end-to-end testing.

- If you cannot do end-to-end testing, then consider live testing of all links possible to help ensure minimum problems.
  - Or, do simulation/modeling
  - Or, do walkthrough

Overall testing may take the form of reviews, analyses, or simulations of contingencies. Reviews and analyses may be used for non-critical systems, whereas critical systems *shall* be tested under conditions that simulate an emergency or a disaster.

It is advisable that the testing of critical systems be done end-to-end, input through output, so that no physical activity, automated process, or Medicare business partner system is left untested. Critical interfaces internal and external to the systems *shall* be tested.

Testing may include activities in addition to computer processing. Manual operations *shall* be checked according to procedures, and changes made as experience indicates.

6.4 Local Processing Environments (PCs/LANs)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

IT systems contingency plan testing relative to local environments, such as individual or clustered workstations and LAN configurations, may be less comprehensive than data center testing. Reviews and analyses may be used to accomplish certain non-critical systems testing, whereas critical systems require full simulation or live testing. The criticality of the system is the deciding factor relative to what type testing is used, how often tests are accomplished, and how thorough the testing *shall* be.

The decision of which test approach to use relative to a specific system or configuration *shall* be a management decision based on advice from the SSO, IT systems staff, operations and support representatives, and the lead test planner/manager.

6.5 Test Planning

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

An IT systems contingency test plan *shall* address at least the following:

- Test objectives
- Test approach

- Required equipment and resources
- Necessary personnel
- Schedules and locations
- Test procedures
- Test results
- Failed tests
- Corrective action management process
- Retest
- Approvals

It is advisable to establish test teams responsible for preparing and executing the IT systems contingency plan tests. Responsibilities *shall* be assigned to test team members, including executives, observers, and contractors.

Following testing, the corrections specified in a Corrective Action Management Process *shall* be tested. The process *shall* include:

- List of items that failed the previous test
- Corrections planned
- Retest detail
- Schedule
- Review responsibilities

Ensure that the lessons learned from IT systems contingency plan testing are discussed among senior business partner management, operations, IT management and staff, and the SSO.

Documentation *shall* exist for:

- Test plans
- Test results
- Corrective action management process
- Retest plans
- Memos of Understanding/Formal Test Arrangements

7 Minimum Recovery Times

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Recovery time is the time it takes to recover an operation, function, process, program, file, or whatever has to be recovered as an operational entity.

Minimum recovery time is the longest acceptable period of time for recovery of operations. If claims processing operations must be recovered within 72 hours, then that is the minimum acceptable time to recover. Anything over that is unacceptable.

- Recovery times *shall* vary, depending on the criticality of the entity involved.
- Times can be from a few minutes to days or weeks.
- A table/matrix can be constructed that lists the recovery times.
- There can be a separate table/matrix for each organization or major function (e.g., claims processing, medical review, check generation).
- Recovery times *shall* be carefully defined and must be achievable.
- Recovery times can be verified to some extent through testing (simulation or live).

8.1 Business Partner Management

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

- Defines scope and purpose of IT systems contingency planning.
- Authorizes preliminary IT systems contingency planning.
- Ensures that appropriate contingency plans are developed, periodically tested, and maintained.
- Ensures that all IT operations participate in the contingency planning and the development of the plans.
- Reviews the plan and recommendations.
- Requests and/or provides funds for plan development and approved recommendations.
- Assigns teams to accomplish development of test procedures, and for testing the plan.
- Reviews test results.
- Ensures that the appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are ready for use in the event of a disruption.
- Ensures that the business partner organization can demonstrate the ability to provide continuity of critical IT systems operation in the event of an emergency.
- Business partner management *shall* approve:

- The Contingency Plan
- Changes to the Contingency Plan
- Test Plans
- Test results
- Corrective action management processes
- Retest Plans
- Memos of Understanding/Formal Arrangement Documents
- Changes to storage and backup/alternate site facilities

9 Changes

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The contingency plan *shall* be updated whenever one or more of the following events occurs:

- New systems or operations added.
- Upgrade or replacement of Standard System software.
- Hardware or software replacement.
- Changed back up/alternate site.
- Changed storage facilities.
- Removal of existing systems or operations.

10 Attachments

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Materials that are too extensive to be included in the body of the Medicare IT systems contingency plan *shall* be included as attachments. These *shall* be referenced in the contingency plan. These *shall* also be a part of the Site Security Profile (Refer to CSR Category 1). Existing material that facilitates response, backup, and recovery operations *shall* be included as attachments or a pointer provided. Much of this material is bulky and relates to the entire organization. The SSO *shall* ensure that the information to be attached is pertinent and current, and that updated copies are routinely incorporated, particularly into offsite copies of the contingency plan. Such material includes:

- Master inventories of forms, supplies, and equipment
- Description of computer hardware and peripherals
- Description of applications software
- Appropriate security weakness information
- Systems and program documentation
- Prioritized schedules for computer operations
- Communications requirements, especially computer networks

11 Checklist

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The following checklist provides a means for determining if a contingency plan contains the appropriate information that can readily be used in handling an emergency or system disruption. This list is not all-inclusive, but rather should serve as a thought stimulus for evaluating contingency plans.

This checklist uses the same outline as the suggested contingency plan format.

1. Introduction
   Does the contingency plan contain:

   - Background
     Is a history of the plan provided? Are the physical environment and the systems discussed?

   - Purpose/Objective
     What does the plan address? Why was it written? What does it aim to accomplish?

   - Management Commitment Statement
     Has the contingency plan been approved by management and the SSO? Once the contingency plan is created, reviewed, and ready for distribution, it *shall* be approved by site, operations and information systems management, and the SSO.

   - Scope
     Are the boundaries of the plan indicated? What organizations are involved, not involved?
     - Organizations
     - Systems
     - Boundaries

   - IT Capabilities and Resources
     Is the focus of the plan on IT systems, capabilities, and resources?

   - Contingency Plan Policy

     - Priorities
       - Are the contingency plan steps ranked according to priority?

     - Continuous Operation
       - Are there functions, processes, or systems that are required to continue without interruption?

- Recovery after Short Interruption
  - Which functions, processes, or systems can be interrupted for a short time?

- Recovery Times?
  - Are the recover times stated?
  - What are the minimum recovery times?

- Standalone Units
  - Does a contingency plan exist for any standalone workstation? A key part of a contingency plan *shall* address any standalone workstations that are part of the critical operations environment. It *shall* state where backup software and support data for these workstations is stored.
  - Is the plan reviewed and approved by other key affected persons?

2. Assumptions
   Are all the important assumptions listed? Have the assumptions been carefully reviewed by the appropriate persons to ensure their validity?

3. Authority/References
   - Who or what document is authorizing the creation of the contingency plan?
   - What are the key references that apply to the plan?

4. Definition of what the Contingency Plan Addresses

   - Organizations
     To which organizations does the contingency plan apply?

   - Systems
     Is there a general description of systems and/or processes?

   - Boundaries
     Are the system boundaries clearly defined?

5. Three phases defined
   Does the plan address three phases of emergency or system disruption?

   - Respond
     - Is this phase adequately described so that it is understood what activities occur therein?
     - Is damage/impact assessment considered?
     - Are the alerting and initial impact assessment procedures fully explained as well as arrangements for continual review of their use and effectiveness?

   - Recover

Is this phase adequately described so that it is understood what activities occur during this phase?

- Restore/Reconstitute
  Is this phase adequately described so that it is understood what activities occur during this phase?

6. Roles/Responsibilities Defined

   - Has the necessary contingency plan implementation organization been defined and the responsibilities of all those involved clearly stated with no 'gray areas'?

   - Will all who have a task to perform be aware of what is expected of them?

   - Does the contingency plan assign responsibilities for recovery? The responsibilities of key management and staff persons *shall* be carefully described in the contingency plan, so that there is no question relative to the duties of these people during an emergency.

7. Definition of Critical Functions

   - Does the contingency plan address critical systems and processes?

   - Have emergency processing priorities been established and approved by management?

   - Does the contingency plan specify critical data? The contingency plan *shall* specify the critical data needed to continue critical business functions and how frequently the data is backed up.

   - Has a list of critical operations, data, and applications been created? In preparation for preparing the contingency plan, a list of current critical operations, data and applications *shall* be prepared and approved by management. This list *shall* contain the items needed to continue the critical business functions until operations could be returned to a normal mode.

8. Alternate Capabilities and Backup

   - Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.

- Does the contingency plan address issues relative to pre-planned alternate locations? The contingency plan *shall* address any potential issues relative to pre-planned alternate locations. These include:
  - insurance
  - equipment replacement
  - phones
  - utilities
  - security

- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities *shall* include:
  - prioritizing operations
  - identifying key personnel and how to reach them
  - listing backup systems and where they are located
  - stocking critical forms, blank check stock, and supplies off-site
  - developing reliable sources for replacing equipment on an emergency basis

- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?

- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?

- Have temporary data storage sites and location of stored backups been identified?

- Is the frequency of file backup documented?

- Have the arrangements been made for ensuring continuing communications capabilities?

- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?

- Are system, application, and other key documentation maintained at the off-site location?

- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?

- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs. These are stored at off-site locations sufficiently distant from the

primary site so as not to be affected by the same emergency that would affect the primary site.

- Is the contingency plan stored off-site at alternate/backup locations? Copies of the contingency plan *shall* be stored at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the contingency plan that are stored in a private home *shall* be protected from inadvertent access.

9. Required Resources

- Are the following resources for supporting critical operations defined and available for an emergency?
  - Hardware
  - Software
  - Communications
  - Data
  - Documents
  - Facilities
  - People
  - Supplies
  - Basic essentials (water, food, shelter, transportation, etc.)

- Does the contingency plan provide for backup personnel? As the contingency plan is implemented, it is necessary to have additional people available to support recovery operations. The contingency plan *shall* specify who these people are and when they would normally be called into action.

10. Training

- Are management and staff trained to respond to emergencies? Security training *shall* include modules for management and staff relative to their roles for handling emergency situations.

11. Testing the Contingency Plan

- Is there a section in the contingency plan that addresses testing of the plan?
- Testing of the contingency plan *shall* address the following topics:
  - Test Philosophy
  - Test Plans
  - Boundaries
  - Live vs. Walkthrough vs. End-to-End Testing
  - Test Reports
  - Responsibilities

12. Contingency Plan Maintenance

- Schedule
  - Is the contingency plan annually reviewed and tested? The contingency plan *shall* be reviewed and tested annually under conditions as close to an emergency as can be reasonably and economically simulated.
  - Is there a provision for updating the contingency plan annually?
  - Is the contingency plan revised after testing, depending on test results?

13. Relationships/Interfaces

- Does the contingency plan identify critical interfaces? Interfaces required to continue critical business functions should be identified. Refer to the System Security Plans.

- Which outside (vendors, providers, banks, utilities, services, CMS) interfaces must be considered?

- Is the plan compatible with plans of interacting organizations and systems?

- What internal interfaces must be considered?

- Is the plan compatible with plans of interacting organizations and systems?

- Which corporate interfaces must be considered?

- Are there special interfaces with corporate systems that must be addressed in the contingency plan?

14. Attachments

Does the contingency plan contain appropriate attachments, as listed below?

A. Actions for Each Phase

Are the actions to be taken in each phase (respond, recover, restore) of the contingency clearly described and related to organizations and/or people?

B. Procedures

- Are there detailed instructions for:
  - responding to emergencies?
  - recovering?
  - restoring operations?

- Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency *shall* be in place.

- Are there procedures for addressing the situation where the processing site is intact, but people can't get to it because of a natural disaster? Can the business be operated remotely?

- Is there an implementation plan for working from home?

C. Call Trees

Are there call lists with names, addresses, and phone numbers with priority order relative to whom to call first?

D. Hardware Inventory

Are there lists of all the hardware covered by the contingency plan?

E. Software Inventory

Are there lists of all the software covered by the contingency plan?

F. System Descriptions

Are all the systems covered by the contingency plan defined, including appropriate diagrams?

G. Alternate/Backup Site Information

Is there sufficient detail to completely describe the alternate and/or backup sites, including addresses, phone numbers, contacts, resources available at the sites, and, resources needed to be brought to the site?

H. Assets/Resources

Are there lists of all the needed resources for responding, recovery, and restoring operations?

I. Risk Assessment Summary

Has there been a realistic assessment of the nature and size of the possible threat and of the resources most at risk?

J. Agreements/Memo of Understanding

Are there agreements in place relative to the use of alternate/backup sites, special resources, outside suppliers, extra people, alternate communications, etc?

K. Manual Operations

Are manual operating procedures in place so that certain functions can continue manually if automated support is not available soon enough?

Manual processing procedures *shall* exist in the backup phase until automated capabilities can take over the information processing. Provisions *shall* be made to provide this manual capability.

L. Supplies/Materials/Equipment

Is there information that describes how and where to obtain needed supplies, materials, and equipment?

M. Floor Plans

Are the necessary floor plans available?

N. Maps

Are the necessary area and street maps available?

12 References

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

In addition to this manual, the following documents may be referenced during the IT systems contingency planning process:

- NIST Special Pub 800-34, Contingency Planning Guide for Information Technology Systems, June 2002. http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 11. http://csrc.nist.gov/publications/nistpubs/800-12

- Health Insurance Portability & Accountability Act (HIPAA): The Race to Become Compliant, Ed Deveau, Disaster Recovery Journal, Fall 2000. http://hipaa.ascensionhealth.org/infoexchange/disaster.html

- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, Section 3.6.

http://www.gao.gov/special.pubs/12_19_6.pdf

- Presidential Decision Directive/NSC 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998. http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004. http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html

- Office of Management & Budget, Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, 8 February 1996. http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

- *CMS Contingency Planning Tabletop Test Procedures, Version 1.1., 25 July 2007. http://www.cms.hhs.gov/informationsecurity/downloads/cp_tabletop_template.zip*

Appendix D:
CMS Information Security *(IS)* Guidebook for Audits

1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This guide has been developed to aid contractors in understanding and preparing for the various types of audits and reviews, which may be performed at their locations. Its purpose is to provide additional information on site selection criteria, audit steps and objectives, documentation requirements, the types of employees that will need to be interviewed, space and equipment requirements for *Chief Financial Officer (*CFO*)/ Electronic Data Processing (EDP)* audits, Section 912 Reviews, *Statement on Auditing Standards (*SAS*) No.* 70 type II audits, and Penetration/*External Vulnerability Assessment (*EVA*)* testing.

1.1 CFO/EDP Audits

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The purpose of these audits is to ensure that proper *information technology (*IT*)* controls exist within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IT controls is needed from each contractor site to determine the sufficiency of overall controls for Centers for Medicare & Medicaid Services (CMS). The level of controls is used to assess the impact of their presence on the financial statements and operations of CMS.

The Chief Financial Officer's Act of 1990 was enacted to improve the general and financial management of the Federal government and established the foundation for the Government Performance Results Act (GPRA). A CFO Act audit is conducted under the guidelines and supervision of the U.S. General Accountability Office (GAO). The GAO requires that all such audits follow the Federal Information Systems Control and Audit Manual (FISCAM). FISCAM includes 6 major areas: Entity-wide Security Program, Access Controls, Application Development and Change Control, Systems Software, Service Continuity, and Segregation of Duties.

1.2 Section 912 Evaluation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

As part of the Medicare Prescription Drug, Improvement and Modernization Act (MMA) of 2003, a requirement exists to perform an evaluation of the information security *(IS)* programs at the Medicare Fiscal Intermediaries and Carriers. The programs at these contractors *shall* be in compliance with the eight statutory requirements *(see below)* set forth in the Federal Information Security Management Act (FISMA).

These evaluations are conducted according to procedures established by the Office of Information Services (OIS) with input from the U.S. Department of Health and Human

Services *(DHHS)*, Office of Inspector General (OIG). The procedures are organized using the eight FISMA statutory areas which include:

1. *P*eriodic *Information Security (IS)* Risk Assessments *(RA)*;
2. *P*olicies and procedures based on *IS RAs* that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the Systems Development Life Cycle (SDLC) and complies with the National Institute of Standards and Technology (NIST) standards;
3. System Security Plans *(SSP)*;
4. *S*ecurity awareness training;
5. *P*eriodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities;
6. *R*emedial activities, processes and reporting for deficiencies;
7. *I*ncident detection, reporting and response*;* and
8. *C*ontinuity of operations for IT systems.

1.4 Penetration/EVA

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the GAO's FISCAM dated January 1999. The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal *government* domain.

A network vulnerability assessment is the systematic examination of an information system to:

- *D*etermine the adequacy of security measures,
- *I*dentify security deficiencies,
- *P*rovide data from which to predict the effectiveness of proposed security measures, and
- *C*onfirm the adequacy of such measures after implementation.

Penetration testing utilizes selected intrusion techniques that may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

2.1 CFO/EDP Audit Acts

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The purpose of these audits is to ensure that proper IT controls exist within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IT controls is needed from each contractor site to determine the sufficiency of overall controls for CMS. The level of controls is used to assess the impact of their presence on the financial statements and operations of CMS.

A CFO Act audit is conducted under the guidelines and supervision of the U.S. GAO. The GAO requires that all such audits follow FISCAM. FISCAM includes 6 major areas: Entity-wide Security Program, Access Controls, Application Development and Change Control, Systems Software, Service Continuity, and Segregation of Duties.

One overall report is created for each site audited with the final report being issued by the OIG.

2.1.1 Site Selection Criteria

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Selection of sites to be included in the CFO Act *a*udit is primarily based on the volume of claims processed, prior findings, and significance of processing done. Smaller sites are rotated into the testing to ensure that their controls are also understood, but such sites are not likely to be audited every year. Because of the new requirements of the security evaluations set forth in Section 912 of the MMA (see section *2.2* of this guide for more detail), the need to rotate smaller sites into testing samples may diminish in the future.

2.1.2 Audit Steps and Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The *DHHS* OIG performs audit work on the following areas of FISCAM during their audits:

Physical Access Controls

- AC-1 Classify information resources according to their criticality and sensitivity.
  - AC-1.1 Resource classifications and related criteria have been established.
  - AC-1.2 Owners have classified resources.

- AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
  - AC-3.1 Adequate physical security controls have been implemented.
    - AC-3.1.A Physical safeguards have been established that are commensurate with the risks of physical damage or access.
    - AC-3.1.B Visitors are controlled.
  - AC-3.4 *Sanitation of e*quipment and media prior to disposal or reuse.

Service Continuity

- SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.
  - SC-1.1 Critical data and operations are identified and prioritized.
  - SC-1.2 Resources supporting critical operations are identified.
  - SC-1.3 Emergency processing priorities are established.

- SC-2 Take steps to prevent and minimize potential damage and interruption.
  - SC-2.1 Data and program backup procedures have been implemented.
  - SC-2.2 Adequate environmental controls have been implemented.
  - SC-2.3 Staff has been trained to respond to emergencies.
  - SC-2.4 Effective hardware maintenance, problem management, and change management *help* prevent unexpected interruptions.

- SC-3 Develop and document a comprehensive contingency plan.
  - SC-3.1 An up-to-date contingency plan is documented.
  - SC-3.2 Arrangements have been made for alternate data processing and telecommunications facilities.

- SC-4 Periodically test the contingency plan and adjust it as appropriate.
  - SC-4.1 The plan is periodically tested.
  - SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly.

The CMS-contracted auditor performs audit work on the following areas of FISCAM as part of the CFO Act audits:

Access Controls

- AC-2 Maintain a current list of authorized users and their access authorized.
  - AC-2.1 Resource owners have identified authorized users and their access authorized.
  - AC-2.2 Emergency and temporary access authorization is controlled.
  - AC-2.3 Owners determine disposition and sharing of data.

- AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
  - AC-3.2 Adequate logical access controls have been implemented. (see also EVA)
    - AC-3.2.A Passwords, tokens, or other devices are used to identify and authenticate users.
    - AC-3.2.B Identification of access paths.
    - AC-3.2.C Logical controls over data files and software programs.
    - AC-3.2.D Logical control over *a* database.
    - AC-3.2.E Logical controls over telecommunications access.
  - AC-3.3 Cryptographic tools. (see also EVA)

- AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.
  - AC-4.1 Audit trails are maintained.
  - AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.

- AC-4.3 Suspicious access activity is investigated and appropriate action is taken.

2.1.4 Documentation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Documentation needed by the OIG for a CFO Act *audit* usually depends on the contractor's role in the Medicare system. This documentation includes, but is not limited to the following:

1. Entity-wide security programs (e.g., *SSP*)
2. Network diagrams
3. *IS RA*s and vulnerability analyses
4. Organizational charts which include names and titles for the Medicare, information systems, and information system security departments
5. *FISMA Evaluation* with Core Set of Security Requirements *(CSR)* using the CMS Integrated Security Suite (CISS)
6. *IS RA* policies and any internal risk analysis documentation
7. Documentation on data and resource classification
8. *Human Resource (*HR*)* policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
9. The most recent SAS 70 and *IS RA* reports
10. Policies and procedures regarding conduct in the data center
11. Policies and procedures for back-up tape rotation and off-site storage
12. Policies and procedures for sanitation of media prior to disposal
13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms
14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas
15. Layout of company buildings and overview of operations in each building

16. Employee lists for Medicare, information systems, and information system security departments (lists *shall* include: name or identification (ID) number, job title, department, start date, and position effective date)

17. Documentation of new hire information system security training program

18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas

19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract

20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests

21. Policies and procedures regarding the testing of the disaster recovery plan

22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable

23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan

Documentation needed by the CMS-contracted auditor for a CFO Act *audit* usually depends on the contractor's role in the Medicare system. This documentation includes, but is not limited to the following:

Application Development and Change Management

Information on change management, including the following:

1. SDLC methodology document

2. A list of all changes made during the current fiscal year

3. Dates of and training materials from the most recent SDLC training class

4. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)

5. A list of all authorized change request approvers

6. Policies and procedures over the use of personal and public domain software

7. Test plan standards

8. A log of *abends*

9. Procedures for new software distribution

10. Policies and procedures for emergency changes

11. A list of all emergency changes during the current fiscal year

12. Identification of virus software in use

13. A list of all users with access to library management software

14. A list of all users with access to the production libraries (production code, source code, extra program copies)

15. Tape library logs for the most recent 3 months

2.1.5 Interviews Required

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer

2. Person responsible for the Corrective Action Plan (CAP)

3. Person responsible for *IS RA*

4. Person responsible for the *SSP*

5. Person in charge of training (entity wide security program)

6. Internal audit lead

7. HR contact

8. Mainframe systems administrator

9. Mainframe security administrator

10. Local Area Network (LAN) administrator

11. Network (LAN) security officer

12. Security software administrator

13. Systems programming manager

14. Person in charge of maintaining the System and Business Continuity Plan

15. Person in charge of the data center

16. Manager of physical security

17. Head of computer operations

18. Person in charge of change management

19. Application manager for the following systems:
    a. Fiscal Intermediary Standard System (FISS)
    b. MultiCarrier System/Mandatory Claim Submission System (MCS)
    c. VIPS Medicare System (VMS)

2.2 Section 912 Evaluation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

As part of the MMA, a requirement exists to perform an evaluation of the *IS* programs at the Medicare Fiscal Intermediaries and Carriers. The programs at these contractors *shall* be in compliance with the eight statutory requirements set forth in the Federal Information Security Management Act (FISMA).

The CMS-contracted auditor has agreed to perform procedures established by CMS and the *DHHS* OIG associated with the eight FISMA statutory areas which include:

1. Periodic *IS RA*s;
2. Policies and procedures based on *IS RA*s that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the systems development life cycle and complies with the NIST standards;
3. System Security Plans;
4. Security awareness training;
5. Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities;
6. Remedial activities, processes and reporting for deficiencies;
7. Incident detection, reporting and response; and
8. Continuity of operations for IT systems.

2.2.2 Audit Steps and Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Risk Assessments

1. Determine if the current system configuration is documented, including links to other systems.

2. Determine if *IS RA*s are performed and documented on an annual basis or whenever the system, facilities, or other conditions change.

3. Determine if data sensitivity and integrity of the data have been documented and if data have been classified.

4. Determine if threat sources, both natural and manmade, have been formally identified.

5. Determine if a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.

6. Determine if an analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.

7. Determine if final risk determinations and related management approvals have been documented and maintained on file.

8. Determine if a mission/business impact analysis have been conducted and documented.

9. Obtain management's list of additional controls that have been identified to mitigate identified risks.

Policies and Procedures to Reduce Risk

1. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in the *IS RA*s section above.

2. Determine if management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.

3. Determine if management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.

4. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.

5. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.

6. Determine if security policies and procedures include controls to address platform security configurations and patch management.

Review of System Security Plans

1. Determine if a security plan is documented and approved.

2. Determine if the plan is kept current.

3. Determine if a security management structure has been established.

4. Determine if *IS* responsibilities are clearly assigned.

5. Determine if owners and users are aware of security policies.

6. Determine if security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications

7. Determine if hiring, transfer, termination, and performance policies address security.

8. Determine if employee background checks are performed.

9. Determine if security employees have adequate security training and expertise.

10. Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.

11. Determine if management ensures that corrective actions are effectively implemented.

Review of Security Awareness Training

1. Determine if employees have received a copy of the Rules of Behavior *(ROB)*.

2. Determine if employee training and professional development has been documented and formally monitored.

3. Determine if there is mandatory annual refresher training for security.

4. Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.

5. Determine if employees have received a copy of or have easy access to agency security procedures and policies.

6. Determine if security professionals have received specific training for their job responsibilities, and if the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.

Review of Periodic Testing and Evaluation of the Effectiveness of IT Security Policies

1. Determine if management reports exist for the review and testing of IT security policies and procedures, including network *IS RA*, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments.

2. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls).

3. Determine if remedial action is being taken for issues noted on audits.

Policies and Procedures for Continuity of Operations and Related Physical Security Safeguards for IT Systems.

1. Determine if critical data and operations are formally identified and prioritized.

2. Determine if resources supporting critical operations are identified in contingency plans.

3. Determine if emergency processing priorities are established.

4. Determine if data and program backup procedures have been implemented.

5. Determine if adequate environmental controls have been implemented.

6. Determine if staff has been trained to respond to emergencies.

7. Determine that hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.

8. Determine if policies and procedures for disposal of data and equipment exist and include applicable *Federal* security and privacy requirements.

9. Determine if an up-to-date contingency plan is documented.

10. Determine if arrangements have been made for alternate data processing and telecommunications facilities.

11. Determine if the contingency plan is periodically tested.

12. Determine if the results are analyzed and the contingency plans are adjusted accordingly.

13. Determine if physical security controls exist to protect IT resources.

2.2.4 Documentation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Documentation needed for Section 912 includes but is not limited to the following areas:

Risk Assessment Review

1. Current system configurations documentation including links to other systems

2. *IS RA*s

3. Data classification policies/procedures

4. Threat source documentation (manmade/natural)

5. Documented system vulnerabilities, system flaws, or weaknesses

6. Risk determinations (assessments) with related management approvals

7. Mission/business impact analysis

System Security Plan

1. *SSP*

2. Security management structure

3. I*S* job responsibilities

4. Hiring, termination, transfer policies/procedures

5. Background check policies/procedures

6. Security policy/procedure updates

7. Management review of corrective actions

2.2.5 Interviews Required

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer

2. Person responsible for the CAP

3. Person responsible for I*S RA*

4. Person responsible for the *SSP*

5. Person in charge of training (entity wide security program)

6. Internal audit lead

7. HR contact

8. Mainframe systems administrator

9. Mainframe security administrator

10. LAN administrator

11. LAN security officer

12. Security software administrator

13. Systems programming manager

14. Person in charge of maintaining the System and Business Continuity Plan

15. Person in charge of the data center

16. Manager of physical security

17. Head of computer operations

18. Person in charge of change management

19. Application manager for the following systems:
    a. FISS
    b. MCS
    c. VMS

2.3 SAS 70 Audits

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

SAS 70, is an internationally recognized auditing standard developed by the AICPA. A SAS 70 audit or service auditor's examination is widely recognized because it indicates that a service organization has been through an in-depth audit of IT control activities and related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting firm. A formal report including the auditor's opinion (Service Auditor's Report) is issued to the service organization at the conclusion of a SAS 70 Audit.

2.3.2 Audit Steps and Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The planned focus of the audit team is collecting information through inquiry, inspection, and observation.

The CMS-contracted auditor will assess the effectiveness of the controls in place as *represented* by management's description of controls. Management's control objectives should be aligned with key FISCAM areas. These key areas include:

- Entity-wide Security Program
- Access Controls
- Control of Application Development and Implementation
- Systems Software
- Service Continuity
- Segregation of Duties

Typically the CMS-contracted auditor will assess the following (and other) control activities; contingent upon them being listed in management's description of controls:

A.1 An entity-wide security program has been documented, approved, and monitored by management in accordance with the CMS Business Partners Systems Security Manual (BPSSM) and includes requirements to assess security risks periodically, establish a security management structure, clearly assign security responsibilities, implement effective security-related personnel

policies, monitor the security program's effectiveness, and ensure security officer training and employee security awareness.

A.2 Security related personnel policies are implemented that include performance of background investigations and contacting references, include confidentiality agreements with employees (regular, contractual, and temporary) and include termination and transfer procedures that require exit interviews, return of property (such as keys and ID cards), notification to security management of terminations, removal of access to systems, and escorting of terminated employees out of the facility.

A.3 Information resources are classified (risk-ranked) according to their criticality/sensitivity and are periodically formally reviewed.

A.4 Access to computerized applications, systems software, and Medicare data are appropriately authorized, documented and monitored, includes approval by resource owners, procedures to control emergency and temporary access and procedures to share and properly dispose of data.

A.5 Security policies and procedures include controls to ensure the security of platform configurations and to ensure proper patch management of operating systems.

A.6 Physical access by all employees (including visitors) to Medicare facilities, data centers, and systems is appropriately authorized, documented, and access violations are monitored and investigated.

A.7 Medicare application and related systems software development and maintenance activities are authorized, documented, tested, and approved.

A.8 A *SDLC* methodology is documented and in use and includes planning for and costs for security requirements in systems.

A.9 Change management policies and procedures exist that include documented testing and approval of changes for regular and emergency changes and restrictions on the use of public domain and personal software.

A.10 Access to program libraries is properly restricted, and movement of programs among libraries is controlled.

A.11 Adequate segregation of duties exists between various functions within Medicare operations and is supported by appropriately authorized and documented policies.

A.12 Activities of employees *shall* be controlled via formal operating procedures that include monitoring of employee activities by management with

documentation maintained to provide evidence of management's monitoring and review process.

A.13 A regular *IS RA* of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated annually. The assessment includes identification of threats, known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.

A.14 A centralized risk management focal point for I*S RA* has been established that includes promotion awareness programs, processes and procedures to mitigate risks and monitoring processes to assess the effectiveness of risk mitigation programs.

A.15 A*n IS RA* and *SSP* has been documented, approved, and monitored by management in accordance with the CMS *Information Security (IS)* Risk Assessment *(RA)* and Systems Security Plan *(SSP) Procedures*.

A.16 Regularly scheduled processes required to support the Medicare contractor's continuity of operations (data, facilities or equipment) are performed.

A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial actions addressing findings noted from all security audits and reviews of IT systems, components and operations.

A.18 Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.

A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts, and actual intrusions.

A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with FISMA.

2.3.4 Documentation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Documentation needed for SAS 70 is specific to the control activities defined by management at each contractor site but may include the following:

1. Entity wide security programs (e.g., *SSP*)
2. Network diagrams
3. *IS RA*s and vulnerability analyses

4. Organizational charts that include names and titles for the Medicare, information systems, and information system security departments

5. Completed CSRs using the CISS

6. *IS RA* policies and any internal risk analysis documentation

7. Documentation on data and resource classification

8. HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations

9. The most recent SAS 70 and *IS RA* reports

10. Policies and procedures regarding conduct in the data center

11. Policies and procedures for back-up tape rotation and off-site storage

12. Policies and procedures for sanitation of media prior to disposal

13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms

14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas

15. Layout of company buildings and overview of operations in each building

16. Employee lists for Medicare, information systems, and information system security departments (lists *shall* include: name or identification (ID) #, job title, department, start date, and position effective date)

17. Documentation of new hire/information system security training program

18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas

19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract

20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests

21. Policies and procedures regarding the testing of the plan

22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable

23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan

24. Security policies, standards, and procedures for:
    a. Creation, modification, and deletion of user-IDs, functional groups, etc.
    b. Periodic review of access
    c. Dial-up access
    d. Use and monitoring of emergency or temporary access (Fire-call IDs)
    e. Password composition/mask
    f. Violation and security monitoring
    g. Archiving, deleting, or sharing data files
    h. Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)

25. List of all terminations during the current fiscal year

26. List of all transfers during the current fiscal year

27. List of all new hires during the current fiscal year

28. List of all Medicare application users

29. List of all users with dial up access

30. List of all users with the ability to change security settings (administrators)

31. Access to access requests and authorizations (for a sample of users)

32. List of access request approvers

33. Documentation supporting recertification of users

34. List of emergency or temporary (fire-call) IDs

35. Activity log of emergency or temporary IDs

36. Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties

37. System default password requirements

38. Use of generic, group or system IDs

39. Database security requirements and settings

40. Security violation logging and monitoring

41. Evidence of review of user templates and/or profiles

42. Evidence of automatic timeout on terminals

43. Database access lists

44. Evidence supporting resolution of prior year audit findings

45. Results of CA_EXAMINE runs

46. Policies and procedures for restricting access to systems software

47. A list of all system programmers

48. A list of all application programmers

49. A list of all computer operators

50. Results of the last review of system programmer access capabilities

51. A list of all vendor supplied software indicating the current version of the software

52. If available, integrity statements from vendors for all third party software

53. Policies and procedures for using and monitoring use of system utilities

54. Policies and procedures for identifying, selecting, installing and modifying systems software

55. Policies and procedures for disabling vender supplied defaults

56. Roles and responsibilities for system programmers

57. Policies and procedures for emergency software changes

58. A list of all systems software changes made during the fiscal year

59. A list of all emergency changes made during the fiscal year

60. A list of all current access to systems software

61. A list of all users with access to migrate programs to production

62. A sample of audit logs for system utilities and system programmer activity

63. Evidence of review of logs and follow up action taken

64. IPL procedures

65. Log from last IPL

66. SDLC methodology document

67. Change control policies and procedures (if not included in the SDLC document)

68. A list of all changes made during the current fiscal year

69. Dates of and training materials from the most recent SDLC training class

70. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)

71. A list of all authorized change request approvers

72. Policies and procedures over the use of personal and public domain software:

73. Test plan standards

74. A log of abends

75. Procedures for new software distribution

76. Policies and procedures for emergency changes

77. A list of all emergency changes during the current fiscal year

78. Identification of virus software in use

79. A list of all users with access to library management software

80. A list of all users with access to the production libraries (production code, source code, extra program copies)

81. Tape library logs for the most recent 3 months

82. Current system configurations documentation including links to other systems

83. Threat source documentation (manmade/natural)

84. Documented system vulnerabilities, system flaws or weaknesses

85. Mission/business impact analysis

86. Job descriptions for management

87. I*S* job responsibilities

88. Background check policies/procedures

89. Security policy/procedure updates

90. Management review of corrective actions

91. Training/professional development policies/procedures

92. Training schedule (if applicable)

93. Awareness posters, booklets, newsletters, etc

94. Management reports for review & testing of IT security policies & procedures

95. Independent audit reports and evaluations

96. Tracking of weaknesses (DB, paper, etc)

97. Planned corrective actions

98. CAP

99. List of IT security weaknesses including dates of corrective actions

100. Policies/procedures for monitoring systems & the network

101. Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions

2.3.5 Interviews Required

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer
2. Person responsible for the CAP
3. Person responsible for I*S RA*
4. Person responsible for the *SSP*
5. Person in charge of training (entity wide security program)
6. Internal audit lead
7. HR contact
8. Mainframe systems administrator
9. Mainframe security administrator
10. LAN administrator
11. LAN security officer
12. Security software administrator
13. Systems programming manager
14. Person in charge of maintaining the System and Business Continuity Plan
15. Person in charge of the data center
16. Manager of physical security
17. Head of computer operations
18. Person in charge of change management
19. Application manager for the following systems:
    a. FISS
    b. MCS
    c. VMS

2.4 Penetration/EVA

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the GAO FISCAM, dated January 1999.

The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal *government* domain.

For purposes of this engagement, a network vulnerability assessment is the systematic examination of an information system, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Penetration testing utilizes selected intrusion techniques that may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

2.4.1 Execution of the Audit

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Due to the sensitive nature of the testing, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results. The testing includes procedures to demonstrate both external and internal threats. To ensure that the integrity of the testing is not impaired, parties with knowledge of the testing are requested to restrict communicating any aspects, including test schedules to individuals at the operational level prior to or during test performance.

The CMS-contracted auditor is the Independent Public Accountant (IPA) engaged by the *DHHS* OIG to perform testing at third party CMS contractors as part of the FY 2004 Financial Statement Audit of CMS. There will be a site summary that includes a high level description of the testing performed and findings describing technical issues identified during testing. The findings will be written in terms of Condition, Cause, Criteria, Effect, and Recommendation (following GAO Yellow Book guidelines). The Site Summary will be supported by summary work papers for each type of testing performed.

2.4.3 Audit Steps and Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Steps to Perform Penetration Testing

Phase 1 – Assess & Model Threats

The Assess & Model Threats phase is used to establish and acquire the information required to successfully define the scope of the security penetration testing. This involves gathering information and completing an initial threat analysis to ensure that testing emulates the threats that are of real concern to the organization. This includes project start-up, information gathering and threat analysis.

1. Threat analysis is usually conducted according to prescribed scenarios that are clearly documented in the Statement of Work. Some common threat scenarios for an external penetration test include:

    a. **Untrusted Outsider** – This is the most common scenario for an External (Internet) penetration test. This scenario is designed to simulate individuals with no significant knowledge of the client's computing operations that are attempting to gain access from remote locations;

    b. **Trusted Outsider** – This scenario is designed to simulate third parties (e.g., customers, suppliers, partners) that have limited legitimate access to the client's network. In the event of the trusted outsider scenario, establish with the client what resources the team will attack and arrange for the client to set up valid credentials to access those resources (e.g., usernames/passwords, SecurID tokens).

2. During the project start-up, agree on primary contacts for both the CMS-contracted auditor and the client to contact in case of an emergency. These contact numbers *shall* be accessible at all times during testing. All members of the team should be aware of the escalation path and procedures during testing.

3. Determine with the client when testing should stop. Some clients request that as soon as access is obtained, the CMS-contracted auditor stop and notify the client before attempting to obtain further access to resources.

4. Determine if there are specific targets of interest that the CMS-contracted auditor should direct attacks to (e.g., a focus on the client's web server).

5. All penetration activities *shall* be conducted from either a CMS-contracted auditor lab or the client site. Identify the source *Internet Protocol (*IP*)* range you will be using with the client to allow them to differentiate the CMS-contracted auditor activities from legitimate hacking attempts. Contact your lab manager for information on your external IP address range.

6. Establish acceptable timeframes for penetration testing with the client to avoid disrupting day-to-day client business (and to avoid being caught if the engagement requires stealth testing).

7. Inquire about any IP addresses that should be excluded from testing.

Phase 2 – Survey Testing

The Survey Testing phase is used to identify and document client devices that may be accessed from the Internet and to determine if any of these devices might be vulnerable to well-known exploits. This includes gathering IP address, MAC address, operating

system, web server, application, and enticement information, in addition to any other salient information about the target environment.

1. Identify Internet connections and IP ranges by querying public databases.

2. Identify salient target information available in newsgroups and web pages.

3. Use DNS queries to identify client networks and systems. These queries are best performed from a UNIX system that has the dig utility installed (NOTE: *D*ig is also available for Windows systems). IP addresses that are found through DNS queries should be looked up in the Internet repositories listed above to determine the range and owner of the IP address. The following queries can be used to identify client systems and networks:

4. Once you have identified client IP ranges and accessible websites, confirm IP addresses with the client contact before attempting to attack any systems.

    a. Once the client has approved the IP ranges identified during the first part of this phase, scans can be conducted using a map to identify open ports and potential attack points on each of the servers in the range. Depending on the requirements of the organization, different types of scans may be used to try and avoid detection.

5. Once the initial scan is complete, a table should be created for the information gathered from each port.

6. After you have identified the services running on each port and obtained all information possible, the Intrusion Testing Phase of the engagement can begin. Note: confirm with the engagement manager before beginning Intrusion testing to determine if the client needs to be notified before beginning.

Phase 3 – Intrusion Testing

The Intrusion Testing phase is used to examine the weaknesses found and, where appropriate, attempt to exploit these weaknesses to demonstrate the risks and exposures. This stage is the core of the security penetration test and may be an iterative process as one exploited weakness may give rise to further exploitation opportunities.

The overall goal of the Intrusion Testing phase is to demonstrate access to systems and the capability to exploit this access further, not necessarily to gain full uncontrolled access to systems, although there may be instances where such access may be permissible.

1. Each attempt you make to gain access to systems (including every username and password combination) ***shall*** **be documented**. There are an infinite number of

avenues to attempt to gain access to a system, but the intrusion attempts should be performed in the following order.

2. If you gain access to a system, **take a screen shot** and **SLOW DOWN**.

3. Navigate the filesystem and attempt to identify any sensitive data files. These may include usernames, passwords or SMTP strings.

4. Use the machine as a "stepping stone" and exploit any trust relationships to compromise additional machines. Determine any network interfaces this system has (e.g., network interface cards) and determine what capabilities the system gives you (e.g., ping internally, telnet). Further system testing, such as this, should be conducted according to the same procedures prescribed so far: (1) Assess and Model Threats; (2) Survey Testing; and (3) Intrusion Testing.

2.4.4 Documentation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Documentation and other items needed for Penetration/EVA includes, but is not limited to:

1. Network Architecture diagrams and descriptions for the performance of internal diagnostic reviews.

2. Site / system password policies

3. Applicable phone number range for dial-up "war-dialing" testing.

4. Applicable IP address spaces for penetration testing.

5. Listing of IP addresses assigned to, or under the purview of the site.

6. Listing of prohibited telephones/systems/networks

7. Standards and Guidelines (Risk Model) for system configuration.

Additional Penetration/EVA Items include:

1. Personnel to observe the penetration and diagnostic testing activities (if desired by the auditee).

2. Permission to connect the CMS-contracted auditor laptop to site's network (while monitored).

3. Network access for internal testing.

System administrator/programmer access for systems to perform diagnostic review.

4. Specific documents required by the CMS-contracted auditor will be requested in the Provided by Client (PBC) list. This list will be provided prior to the start of testing.

3 Tables

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This table provides a synopsis of required documentation.

Table D-1. Synopsis of Documentation Required

Documentation	CFO Audit	Section 912	SAS 70	EVA
Entity wide security programs (e.g., *SSP*)	✔	✔	✔	
Network diagrams	✔	✔	✔	✔
*IS RA*s and vulnerability analyses	✔	✔	✔	
Organizational charts which include names and titles for the Medicare, information systems, and information system security departments	✔	✔	✔	
Completed CSRs using the CISS	✔	✔	✔	
IS RA policies and any internal risk analysis documentation	✔	✔	✔	
Documentation on data and resource classification	✔	✔	✔	
HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations	✔	✔	✔	
The most recent SAS 70 and *IS RA* reports	✔		✔	
Policies and procedures regarding conduct in the data center	✔		✔	
Policies and procedures for back-up tape rotation and off-site storage	✔	✔	✔	
Policies and procedures for sanitation of media prior to disposal	✔	✔	✔	
Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms	✔		✔	
Policies and procedures regarding visitors to both the general campus and to the sensitive areas	✔		✔	
Layout of company buildings and overview of operations in each building	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Employee lists for Medicare, information systems, and information system security departments (lists *shall* include: name or identification (ID) #, job title, department, start date, and position effective date)	✔	✔	✔	
Documentation of new hire/information system security training program	✔	✔	✔	
Vendor sign in and sign out logs for maintenance or repairs in sensitive areas	✔		✔	
Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract	✔		✔	
Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.	✔	✔	✔	
Policies and procedures regarding the testing of the plan	✔	✔	✔	
Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable	✔	✔	✔	
Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan	✔	✔	✔	
Security policies, standards, and procedures for:				
• Creation, modification, and deletion of user-IDs, functional groups, etc.	✔		✔	
• Periodic review of access	✔		✔	
• Dial-up access	✔		✔	
• Use and monitoring of emergency or temporary access (Fire-call IDs)	✔		✔	
• Password composition/mask	✔		✔	✔
• Violation and security monitoring	✔		✔	
• Archiving, deleting, or sharing data files	✔		✔	
• Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)	✔		✔	
List of all terminations during the current fiscal year	✔		✔	
List of all transfers during the current fiscal year	✔		✔	
List of all new hires during the current fiscal year	✔		✔	
List of all Medicare application users/	✔	✔	✔	
List of all users with dial up access	✔		✔	
List of all users with the ability to change security settings (administrators)	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Access to access requests and authorizations (for a sample of users)	✔		✔	
List of access request approvers	✔		✔	
Documentation supporting recertification of users	✔		✔	
List of emergency or temporary (fire-call) IDs	✔		✔	
Activity log of emergency or temporary IDs	✔		✔	
Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties	✔		✔	
System default password requirements	✔		✔	
Use of generic, group or system IDs	✔		✔	
Database security requirements and settings	✔		✔	
Security violation logging and monitoring	✔		✔	
Evidence of review of user templates and/or profiles	✔		✔	
Evidence of automatic timeout on terminals	✔		✔	
Database access lists	✔		✔	
Evidence supporting resolution of prior year audit findings	✔		✔	
Results of CA_EXAMINE runs	✔		✔	
Policies and procedures for restricting access to systems software	✔		✔	
A list of all system programmers	✔		✔	
A list of all application programmers	✔		✔	
A list of all computer operators	✔		✔	
Results of the last review of system programmer access capabilities	✔		✔	
A list of all vendor supplied software that indicates how current the software is	✔		✔	
If available, integrity statements from vendors for all third party software	✔		✔	
Policies and procedures for using and monitoring use of system utilities	✔		✔	
Policies and procedures for identifying, selecting, installing and modifying systems software	✔		✔	
Policies and procedures for disabling vender supplied defaults	✔		✔	
Roles and responsibilities for system programmers	✔		✔	✔
Policies and procedures for emergency software changes	✔		✔	
A list of all systems software changes made during the fiscal year	✔		✔	
A list of all emergency changes made during the fiscal year	✔		✔	
A list of all current access to systems software	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
A list of all users with access to migrate programs to production	✔		✔	
A sample of audit logs for system utilities and system programmer activity	✔		✔	
Evidence of review of logs and follow up action taken	✔		✔	
IPL procedures	✔		✔	
Log from last IPL	✔		✔	
SDLC methodology document	✔	✔	✔	
Change control policies and procedures (if not included in the SDLC document)	✔		✔	
A list of all changes made during the current fiscal year	✔		✔	
Dates of and training materials from the most recent SDLC training class	✔		✔	
Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)	✔		✔	
A list of all authorized change request approvers	✔		✔	
Policies and procedures over the use of personal and public domain software:	✔		✔	
Test plan standards	✔		✔	
A log of *abends*	✔		✔	
Procedures for new software distribution	✔		✔	
Policies and procedures for emergency changes	✔		✔	
A list of all emergency changes during the current fiscal year	✔		✔	
Identification of virus software in use	✔		✔	
A list of all users with access to library management software	✔		✔	
A list of all users with access to the production libraries (production code, source code, extra program copies)	✔		✔	
Tape library logs for the most recent 3 months	✔		✔	
Current system configurations documentation including links to other systems		✔	✔	
Threat source documentation (manmade/natural)		✔	✔	
Documented system vulnerabilities, system flaws or weaknesses		✔	✔	
Mission/business impact analysis		✔	✔	
Job descriptions for management		✔	✔	
I*S* job responsibilities		✔	✔	
Background check policies/procedures		✔	✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Security policy/procedure updates		✔	✔	
Management review of corrective actions		✔	✔	
Training/professional development policies/procedures		✔	✔	
Training schedule (if applicable)		✔	✔	
Awareness posters, booklets, newsletters, etc		✔	✔	
Management reports for review & testing of IT security policies & procedures		✔	✔	
Independent audit reports and evaluations		✔	✔	
Tracking of weaknesses (DB, paper, etc)		✔	✔	
Planned corrective actions		✔	✔	
All four quarter CAPs		✔	✔	
List of IT security weaknesses including dates of corrective actions		✔	✔	
Policies/procedures for monitoring systems & the network		✔	✔	
Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions		✔	✔	
Network Architecture diagrams and descriptions for the performance of internal diagnostic reviews.				✔
Standards and Guidelines (Risk Model) for system configuration.				✔
Applicable phone number range for dial-up “war-dialing” testing.				✔
Applicable IP address spaces for penetration testing.				✔
Listing of IP addresses assigned to, or under the purview of the site.				✔
Listing of prohibited telephones/systems/networks				✔

Table D-2. Detailed CFO Testing Procedures

Control Activity	Detailed Testing
Access Control	
AC-1 Classify information resources according to their criticality and sensitivity.	
1. Resource classifications and related criteria have been established.	1. Review policies and procedures.
	2. Interview resource owners.
2. Owners have classified resources.	1. Review resource classification documentation and compare to *RA*s. Discuss any discrepancies with appropriate officials.
AC-3 Establish physical and logical controls to prevent or detect unauthorized access.	
1. Adequate physical security controls have been implemented.	
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	1. Review a diagram of the physical layout of the computer, telecommunications, and cooling system facilities.
	2. Walk through facilities.
	3. Review risk analysis.
	4. Review lists of individuals authorized access to sensitive areas and determine the appropriateness for access.
	5. Before becoming recognized as the auditor, attempt to access sensitive areas without escort or identification badges.
	6. Observe entries to and exits from facilities during and after normal business hours.
	7. Observe utilities access paths.
	8. Interview management.
	9. Observe entries to and exits from sensitive areas during and after normal business hours.
	10. Interview employees.
	11. Review procedures for the removal and return of storage media from and to the library.
	12. Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was obtained for the movement.
	13. Observe practices for safeguarding keys and other devices.
	14. Review written emergency procedures.
	15. Examine documentation supporting prior fire drills.
	16. Observe a fire drill.
B. Visitors are controlled.	1. Review visitor entry logs.
	2. Observe entries to and exits from sensitive areas during and after normal business hours.
	3. Interview guards at facility entry.

Control Activity	Detailed Testing
	4. Review documentation on and logs of entry code changes.
	5. Observe appointment and verification procedures for visitors.
2. Sanitation of equipment and media prior to disposal or reuse.	1. Review written procedures.
	2. Interview personnel responsible for clearing equipment and media.
	3. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and software.
	4. For selected items still in the entity's possession, test that they have been appropriately sanitized.
Entity Wide Security Program	
SP-1 Risks are periodically assessed.	
1. Risks are periodically assessed.	1. Review *RA* policies.
	2. Review the most recent high-level *RA*.
	3. Review the objectivity of personnel who performed and reviewed the assessment.
SP-2 Document an entitywide security program plan.	
1. A security plan is documented and approved.	1. Review the security plan.
	2. Determine whether the plan covers the topics prescribed by OMB Circular A-130.
2. The plan is kept current.	1. Review the security plan and any related documentation indicating that it has been reviewed and updated and is current.
SP-3 Establish a security management structure and clearly assign security responsibilities.	
1. A security management structure has been established.	1. Review the security plan and the entity's organization chart.
	2. Interview security management staff.
	3. Review pertinent organization charts and job descriptions.
	4. Interview the security manager.
2. I*S* responsibilities are clearly assigned.	1. Review the security plan.
3. Owners and users are aware of security policies.	1. Review documentation supporting or evaluating the awareness program. Observe a security briefing.
	2. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities.
	3. Review memos, electronic mail files, or other policy distribution mechanisms.
	4. Review personnel files to test whether security awareness statements are current.

Control Activity	Detailed Testing
	5. Call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password.
4. An incident response capability has been implemented.	1. Interview security manager, response team members, and system users.
	2. Review documentation supporting incident handling activities.
	3. Determine qualifications of response team members.
SP-4 Implement effective security-related personnel policies.	
1. Hiring, transfer, termination, and performance policies address security.	1. Review hiring policies.
	2. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.
	3. Review reinvestigation policies.
	4. For a selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed.
	5. Review policies on confidentiality or security agreements.
	6. For a selection of such users, determine whether confidentiality or security agreements are on file.
	7. Review vacation policies.
	8. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year.
	9. Determine who performed vacationing employee's work during vacation.
	10. Review job rotation policies.
	11. Review staff assignment records and determine whether job and shift rotations occur.
	12. Review pertinent policies and procedures.
	13. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.
	14. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.
2. Employees have adequate training and expertise.	1. Review job descriptions for security management personnel, and for a selection of other personnel.

Control Activity	Detailed Testing
	2. For a selection of employees, compare personnel records on education and experience with job descriptions.
	3. Review training program documentation.
	4. Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.
SP-5 Monitor the security program's effectiveness and make changes as needed.	
1. Management periodically assesses the appropriateness of security policies and compliance with them.	1. Review the reports resulting from recent assessments, including the most recent FMFIA report.
	2. Determine when the last independent review or audit occurred and review the results.
	3. Review written authorizations or accreditation statements.
	4. Review documentation related to corrective actions.
2. Management ensures that corrective actions are effectively implemented.	1. Review the status of prior-year audit recommendations and determine if implemented corrective actions have been tested.
	2. Review recent FMFIA reports.
Segregation of Duties	
SD-1 Segregate incompatible duties and establish related policies.	
1. Incompatible duties have been identified and policies implemented to segregate these duties.	1. Review pertinent policies and procedures.
	2. Interview selected management and *IS* personnel regarding segregation of duties.
	3. Review an agency organization chart showing *IS* functions and assigned personnel.
	4. Interview selected personnel and determine whether functions are appropriately segregated.
	5. Determine whether the chart is current and each function is staffed by different individuals.
	6. Review relevant alternate or backup assignments and determine whether the proper segregation of duties is maintained.
	7. Observe activities of personnel to determine the nature and extent of compliance with the intended segregation of duties.
	8. Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combination of functions.
	9. Interview management, observe activities, and test transactions.

Control Activity	Detailed Testing
	10. Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.
	11. Review the adequacy of documented operating procedures for the data center.
2. Job descriptions have been documented.	1. Review job descriptions for several positions in organizational units and for user security administrators.
	2. Determine whether duties are clearly described and prohibited activities are addressed.
	3. Review the effective dates of the position descriptions and determine whether they are current.
	4. Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	5. Review job descriptions and interview management personnel.
3. Employees understand their duties and responsibilities.	1. Interview personnel filling positions for the selected job descriptions (see above). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	2. Determine from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	3. Interview management personnel in these activities.
SD-2 Establish access controls to enforce segregation of duties.	
1. Physical and logical access controls have been established.	1. Interview management and subordinate personnel.
2. Management reviews effectiveness of control techniques.	1. Interview management and subordinate personnel.
	2. Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).
	3. Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review the results of such reviews.
SD-3 Control personnel activities through formal operating procedures and supervision and review.	
1. Formal procedures guide	1. Review manuals.

Control Activity	Detailed Testing
personnel in performing their duties.	2. Interview supervisors and personnel. 3. Observe processing activities.
2. Active supervision and review are provided for all personnel.	1. Interview supervisors and personnel. 2. Observe processing activities. 3. Review history log reports for signatures indicating supervisory review. 4. Determine who is authorized to perform the *IPL* for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determine whether operators override the IPL parameters.
Service Continuity	
SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.	
1. Critical data and operations are identified and prioritized.	1. Review related policies. 2. Review list and any related documentation. 3. Interview program, data processing, and security administration officials. Determine their input and their assessment of the reasonableness of priorities established.
2. Resources supporting critical operations are identified.	1. Review related documentation. 2. Interview program and security administration officials.
3. Emergency processing priorities are established.	1. Review related policies. 2. Review related documentation. 3. Interview program and security administration officials.
SC-2 Take steps to prevent and minimize potential damage and interruption.	
1. Data and program backup procedures have been implemented.	1. Review written policies and procedures for backing up files. 2. Compare inventory records with the files maintained off-site and determine the age of these files. 3. For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports. 4. Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned. 5. Locate and examine documentation. 6. Examine the backup storage site.
2. Adequate environmental controls have been	1. Examine the entity's facilities 2. Interview site managers.

Control Activity	Detailed Testing
implemented.	3. Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency.
	4. Observe the operation, location, maintenance and access to the air-cooling system.
	5. Observe whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor.
	6. Determine whether the activation of heat and smoke detectors will notify the fire department.
	7. Review test policies.
	8. Review documentation supporting recent tests of environmental controls.
	9. Review policies and procedures regarding employee behavior.
	10. Observe employee behavior.
3. Staff has been trained to respond to emergencies.	1. Interview data center staff.
	2. Review training records.
	3. Review training course documentation.
	4. Review emergency response procedures.
	5. Review test policies.
	6. Review test documentation.
	7. Interview data center staff.
4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	1. Review policies and procedures.
	2. Interview data processing and user management.
	3. Review maintenance documentation.
	4. Interview data center management.
	5. Interview senior management, data processing management, and user management.
	6. Review supporting documentation.
SC-3 Develop and document a comprehensive contingency plan.	
1. An up-to-date contingency plan is documented.	1. Review the contingency plan and compare its provisions with the most recent *RA* and with a current description of automated operations.
	2. Interview senior management, data center management, and program managers.
	3. Review the contingency plan.
	4. Interview senior management, data center management, and program managers.
	5. Observe copies of the contingency plan held off-site.

Control Activity	Detailed Testing
	6. Review the plan and any documentation supporting recent plan reassessments.
2. Arrangements have been made for alternate data processing and telecommunications facilities.	1. Review contracts and agreements.
SC-4 Periodically test the contingency plan and adjust it as appropriate.	
1. The plan is periodically tested.	1. Review policies on testing.
	2. Review test results.
	3. Observe a disaster recovery test.
2. Test results are analyzed and contingency plans are adjusted accordingly.	1. Review final test report.
	2. Interview senior managers to determine if they are aware of the test results.
	3. Review any documentation supporting contingency plan adjustments.

The CMS-contracted auditor will perform audit work on the following areas of FISCAM as part of the CFO Act audits:

Control Activity	Detailed Testing
Access Controls	
AC-2 Maintain a current list of authorized users and their access authorized.	
1. Resource owners have identified authorized users and their access authorized.	1. Review pertinent written policies and procedures.
	2. For a selection of users (both application user and *IS* personnel) review access authorization documentation.
	3. Interview owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner.
	4. For a selection of users with dial-up access, review authorization and justification.
	5. Interview security managers and review documentation provided to them.
	6. Review a selection of recent profile changes and activity logs.
	7. Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.
2. Emergency and temporary access authorization is controlled.	1. Review pertinent policies and procedures.
	2. Compare a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.

Control Activity	Detailed Testing
	3. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
3. Owners determine disposition and sharing of data.	1. Examine standard approval forms.
	2. Interview data owners.
	3. Examine documents authorizing file sharing and file sharing agreements.
AC-3 Establish physical and logical controls to prevent or detect unauthorized access.	
1. Adequate logical access controls have been implemented. (see also EVA)	
A. Passwords, tokens, or other devices are used to identify and authenticate users.	1. Review pertinent policies and procedures.
	2. Interview users.
	3. Review security software password parameters.
	4. Observe users keying in passwords.
	5. Attempt to log on without a valid password; make repeated attempts to guess passwords.
	6. Assess procedures for generating and communicating passwords to users.
	7. Review a system-generated list of current passwords.
	8. Search password file using audit software.
	9. Attempt to log on using common vendor supplied passwords.
	10. Interview users and security managers.
	11. Review a list of IDs and passwords.
	12. Repeatedly attempt to log on using invalid passwords.
	13. Review security logs.
	14. Review pertinent policies and procedures.
	15. Review documentation of such comparisons.
	16. Interview security managers.
	17. Make comparison using audit software.
	18. View dump of password files (e.g., hexadecimal printout).
	19. Interview users.
	20. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor should obtain the assistance of a specialist.
B. Identification of access paths.	1. Review access path diagram.
C. Logical controls over data files and software programs.	1. Interview security administrators and system users.
	2. Review security software parameters.
	3. Observe terminals in use.

Control Activity	Detailed Testing
	4. Review a system-generated list of inactive logon IDs, and determine why access for these users has not been terminated.
	5. Determine library names for sensitive or critical files and libraries and obtain security reports of related access rules. Using these reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorized.
	6. Perform penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system. These tests should be performed as (1) an "outsider" with no information about the entity's computer systems; and (2) an "outsider" with prior knowledge about the systems--e.g., an ex-insider, and (3) an "insider" with and without specific information about the entity's computer systems, and with access to the entity's facilities.
	7. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
	8. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords.
	9. Determine whether naming conventions are used.
D. Logical controls over a database.	1. Review pertinent policies and procedures.
	2. Interview database administrator.
	3. Review DBMS and DD security parameters.
	4. Test controls by attempting access to restricted files.
	5. Review security system parameters.
E. Logical controls over telecommunications access.	1. Review pertinent policies and procedures.
	2. Review parameters set by communications software or teleprocessing monitors.
	3. Test telecommunications controls by attempting to access various files through communications networks.

Control Activity	Detailed Testing
	4. Identify all dial-up lines through automatic dialer software routines and compare with known dial-up access. Discuss discrepancies with management.
	5. Interview telecommunications management staff and users.
	6. Review pertinent policies and procedures.
	7. View the opening screen seen by telecommunication system users.
	8. Review the documentation showing changes to dial-in numbers.
	9. Review entity's telephone directory to verify that the numbers are not listed.
2. Cryptographic tools. (see also EVA)	1 To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.	
1. Audit trails are maintained.	1. Review security software settings to identify types of activity logged.
2. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Review pertinent policies and procedures.
	2. Review security violation reports.
	3. Examine documentation showing reviews of questionable activities.
3. Suspicious access activity is investigated and appropriate action is taken.	1. Test a selection of security violations to verify that follow-up investigations were performed and to determine what action were taken against the perpetrator.
	2. Interview senior management and personnel responsible for summarizing violations.
	3. Review any supporting documentation.
	4. Review policies and procedures and interview appropriate personnel.
	5. Review any supporting documentation.
Application Software Development and Change Control	
CC-1 Processing features and program modifications are properly authorized.	
1. A SDLC has been implemented.	1. Review SDLC methodology.
	2. Review system documentation to verify that SDLC methodology was followed.
	3. Interview staff.
	4. Review training records.
2. Authorizations for software modifications are documented and maintained.	1. Identify recent software modifications and determine whether change request forms were used.
	2. Examine a selection of software change request forms for approvals.
	3. Interview software development staff.

Control Activity	Detailed Testing
3. Use of public domain and person software is restricted.	1. Review pertinent policies and procedures.
	2. Interview users and data processing staff.
CC-2 Test and approve all new and revised software.	
1. Changes are controlled as programs progress through testing to final approval.	1. Review test plan standards.
	2. For the software change requests selected for control activity CC-1.2: (1) review specifications; (2) trace changes from code to design specifications; (3) review test plans; (4) compare test documentation with related test plans; (5) analyze test failures to determine if they indicate ineffective software testing; (6) review test transactions and data*; (7) review test results; (8) review documentation of management or security administrator reviews; (9) verify user acceptance; and (10) review updated documentation.*.
	3. Determine whether operational systems experience a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
2. Emergency changes are promptly tested and approved.	1. Review procedures.
	2. For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.
3. Distribution and implementation of new or revised software is controlled.	1. Examine procedures for distributing new software.
	2. Examine implementation orders for a sample of changes.
CC-3 Control software libraries.	
1. Programs are labeled and inventoried.	1. Review pertinent policies and procedures.
	2. Interview personnel responsible for library control.
	3. Examine a selection of programs maintained in the library and assess compliance with prescribed procedures.
	4. Determine how many prior versions of software modules are maintained.
2. Access to program libraries is restricted.	1. Examine libraries in use.
	2. Interview library control personnel.
	3. Examine libraries in use.
	4. Verify that source code exists for a selection of production load modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load modules size.
	5. For critical software production programs, determine whether access control software rules are clearly defined.

Control Activity	Detailed Testing
	6. Test access to program libraries by examining security system parameters.
	7. Select some program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.
3. Movement of programs and data among libraries is controlled.	1. Review pertinent policies and procedures.
	2. For a selection of program changes, examine related documentation to verify that: (1) procedures for authorizing movement among libraries were followed, and (2) before and after images were compared.
Systems Software	
SS-1 Limit access to systems software.	
1. Access authorizations are appropriately limited.	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel regarding access restrictions.
	3. Observe personnel accessing systems software, such as sensitive utilities, and note the controls encountered to gain access.
	4. Attempt to access the operating system and other systems software.
	5. Select some systems programmers and determine whether management-approved documentation supports their access to systems software.
	6. Select some application programmers and determine whether they are not authorized access.
	7. Determine the last time the access capabilities of system programmers were reviewed.
2. All access paths have been identified and controls implemented to prevent or detect access for all paths.	1. Test the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls.
	2. Obtain a list of vendor-supplied software and determine if any of these products have known deficiencies that adversely impact the operating system integrity controls.
	3. Judgmentally review the installation of systems software components and determine whether they were appropriately installed to preclude adversely impacting operating system integrity controls.
	4. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods including:

Control Activity	Detailed Testing
	(1) Determine whether the operating system's subsystems have been appropriately implemented to ensure that they support integrity controls.
	(2) Determine whether applications interfaces have been implemented to support operating system integrity controls, including on-line transaction monitors; database software; on-line editors; on-line direct-access storage devices, on-line operating system datasets; exits related to the operating system, security, and program products; and controls over batch processing, to include security controls, scheduler controls, and access authorities.
	(3) Evaluate the controls over external access to computer resources including networks, dial-up, LAN, WAN, RJE, and the Internet.
	(4) Identify potential opportunities to adversely impact the operating system and its products through trojan horses, viruses, and other malicious actions.
	5. Obtain a list of all systems software on test and production libraries used by the entity.
	6. Verify that access control software restricts access to systems software.
	7. Using security software reports, determine who has access to systems software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they *shall* be generated *in* the presence of the auditor.
	8. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
	9. Inquire as to whether disabling has occurred.
	10. Test for default presence using vendor standard IDs and passwords.
	11. Determine what terminals are set up as master consoles and what controls exist over them.
	12. Test to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.
SS-2 Monitor access to and use of systems software.	
1. Policies and techniques have	1. Review pertinent policies and procedures.

Control Activity	Detailed Testing
been implemented for using and monitoring use of system utilities.	2. Interview management and systems personnel regarding their responsibilities.
	3. Determine whether logging occurs and what information is logged.
	4. Review logs.
	5. Using security software reports, determine who can access the logging files.
2. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interview technical management regarding their reviews of privileged systems software and utilities usage.
	2. Review documentation supporting their reviews.
	3. Interview management and systems personnel regarding these investigations.
	4. Review documentation supporting these investigations.
	5. Interview systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Review documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interview management and analyze their reviews concerning the use of systems software.
	8. Determine what management reviews have been conducted, and their currency, over this area.
SS-3 Control systems software changes.	
1. Systems software changes are authorized, tested, and approved before implementation.	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel.
	3. Review procedures for identifying and documenting systems software problems.
	4. Interview management and systems programmers.
	5. Review the causes and frequency of any recurring systems software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.
	6. Determine what authorizations and documentation are required prior to initiating systems software changes.
	7. Select recent systems software changes and determine whether the authorization was obtained and the change is supported by a change request document.
	8. Determine the procedures used to test and approve systems software prior to its implementation.

Control Activity	Detailed Testing
	9. Select recent systems software changes and test whether the indicated procedures were in fact used.
	10. Review procedures used to control and approve emergency changes.
	11. Select some emergency changes to systems software and test whether the indicated procedures were in fact used.
2. Installation of systems software is documented and reviewed.	1. Interview management and systems programmers about scheduling and giving advance notices when systems software is installed.
	2. Review recent installations and determine whether scheduling and advance notification did occur.
	3. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.
	4. Interview management, systems programmers, and library control personnel, and determine who migrates approved systems software to production libraries and whether outdated versions are removed from production libraries.
	5. Review supporting documentation for some systems software migrations and the removal of outdated versions from production libraries.
	6. Interview data center management about their role in reviewing systems software installations.
	7. Review some recent systems software installations and determine whether documentation shows that logging and management review occurred.
	8. Interview systems software personnel concerning a selection of systems software and determine the extent to which the operating version of the systems software is currently supported by the vendor.
	9. Interview management and systems programmers about the currency of systems software and the currency and completeness of software documentation.
	10. Review documentation and test whether recent changes are incorporated.

Table D-3. Detailed MMA 912 Testing Procedures

Control Activity	Detailed Testing
Section I: Risk Assessment Review	
A. Determine if the current system configuration is documented, including links to other systems.	1. Review the most recent system configuration
	2. Review the system configuration and/or related documentation indicating it has been reviewed and kept current
B. Determine if *RA*s are performed and documented on an annual basis or whenever the system, facilities, or other conditions change.	1. Review the *RA* policies
	2. Review the most recent *RA*
	3. Review the *RA* and/or related documentation indicating it has been reviewed and conducted annually
C. Determine if data sensitivity and integrity of the data have been documented and if data has been classified	1. Review data classification policies and procedures
	2. Review evidence based on policies and procedures that data has been classified
D. Determine if threat sources, both natural and manmade, have been formally identified	1. Review *RA* to ensure that threat sources, both natural and man-made, have been identified and documented.
E. Determine if a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.	1. Review the *RA* to ensure that a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed.
	2. Review the *RA* and/or related documentation indicating it has been reviewed and kept current.
F. Determine if an analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.	1. Review the *RA* to ensure that mitigating controls are documented.
	2. Review the *RA* to ensure that mitigating controls have been assessed and documented to determine if they adequately mitigate vulnerabilities.
G. Determine if final risk determinations and related management approvals have been documented and maintained on file.	1. Review the *RA* to ensure that final risk determinations are documented.
	2. Review *RA* and/or related documentation indicating it has been approved (currently).
H. Determine if a mission/business impact analysis have been conducted and documented.	1. Review documented critical business processes.
	2. Review mission/business impact analysis to ensure that it has been documented for the critical business processes
I. Obtain management's list of additional controls that have been identified to mitigate identified risks.	1. Review any additional documented lists of controls identified to mitigate identified risks.
Section II: Policies and Procedures to Reduce Risk	

Control Activity	Detailed Testing
A. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	1. Review the most current *RA*. 2. Review IT Security policies and procedures to ensure that they reduce the risk outlined in the *RA*. 3. Ensure that IT Security policies and procedures are current.
B. Determine if management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	1. Review the most current *SDLC*. 2. Review additional information (i.e., *SSP*) which outline security controls included in the cost of developing new systems 3. Review software change control policies and procedures to ensure that changes are being controlled effectively.
C. Determine if management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	1. Perform inquiries of appropriate personnel regarding major systems maintained at the site. 2. Review documentation indicating accreditations and certifications were performed for the noted systems. 3. Ensure that accreditations and certifications are in compliance with FISMA policies .
D. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.	1. Perform inquiries of appropriate personnel regarding systems for which controls have been tested. 2. Review evidence (i.e., internal/external audits) indicating system controls have been tested and evaluated for the identified systems. 3. Review evidence (i.e., internal/external penetration tests, etc) indicating system/network boundaries have been subjected to periodic reviews/audits. 4. Ensure that all reviews have been performed within the scope of the review.
E. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.	1. Review the most recent CMS CSR. 2. GAPs in compliance as documented in the CMS CSR. 3. Review management's response to the CSR to ensure that proper controls are in place/are in the process of being in place.
F. Determine if security policies and procedures include controls to address platform security configurations, and patch management.	1. Review platform security configuration policies and procedures. 2. Review patch management policies and procedures.
Section III: Review of System Security Plans	

Control Activity	Detailed Testing
A. Determine if a security plan is documented and approved.	1. Review most current *SSP*.
	2. Review documentation indicating the *SSP* was approved by appropriate individuals.
B. Determine if the plan is kept current.	1. Review previous and current *SSP* to ensure that updates have been made as necessary.
	2. Review the date of the most current *SSP* to ensure that it is in the scope of the review.
C. Determine if a security management structure has been established.	1. Review the security management's organizational chart.
D. Determine if *IS* responsibilities are clearly assigned.	1. Review the security management's organization chart.
	2. Review the security management's formal job descriptions.
E. Determine if owners and users are aware of security policies.	1. Review security training schedules.
	2. Review security training materials.
	3. For a selection of owners and users ensure that they have attended the required trainings.
F. Determine if security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	1. Review the most current *SDLC*.
	2. Review additional *SDLC* policies and procedures to ensure that security polices and procedures have been incorporated.
	3. Perform inquiries of appropriate personnel regarding major systems maintained at the site
	4. Review documentation indicating accreditations and certifications were performed for the noted systems.
G. Determine if hiring, transfer, termination and performance policies address security.	1. Review hiring policies and procedure to ensure that they address security.
	2. Review transfer policies and procedures to ensure that they address security.
	3. Review termination policies and procedures to ensure that they address security.
	4. Review performance policies and procedures (i.e., R*OB* and Performance Evaluations) to ensure they address security.
H. Determine if employee background checks are performed.	1. Review policies and procedures for performing background checks.
	2. Select a sample of employees and ensure that background investigations have been completed.
I. Determine if security employees have adequate	1. Identify all employees responsible for administering security.

Control Activity	Detailed Testing
security training and expertise.	2. Review training records and certifications for all security employees to ensure that adequate training has been received.
J. Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Review policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	2. Review documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
K. Determine if management ensures that corrective actions are effectively implemented.	1. Review policies and procedures for ensuring that corrective actions are effectively implemented.
	2. Review evidence that management ensures that corrective actions are effectively implemented.
Section IV: Review of Security Awareness Training	
A. Determine if employees have received a copy of the *ROB*.	1. Inquire of the appropriate personnel regarding the maintenance and distribution of the *ROB* for all types of employees.
	2. Review the most current version of the *ROB*.
	3. Select a sample of employees and ensure that they have received a copy of the most current version of the *ROB*.
B. Determine if employee training and professional development has been documented and formally monitored.	1. Inquire of the appropriate personnel regarding the documentation and formal monitoring of employee training and professional development.
	2. Review policies and procedures regarding the documentation and formal monitoring of employee training and professional development.
	3. For a selected sample of employees, review evidence that training and professional development is documented and formally monitored.
C. Determine if there is mandatory annual refresher training for security.	1. Review policies and procedures regarding mandatory annual refresher security training.
	2. Review the most recent security awareness training curriculum.
	3. For a selected sample of employees, review evidence that all attended the mandatory annual refresher security training.
D. Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.	1. Review policies and procedures regarding methods to make employees aware of security.
	2. Conduct a walk through of the site to ensure that posters/flyers are in fact hanging in visible areas.
	3. Inspect evidence that methods to make employees aware of security are implemented.

Control Activity	Detailed Testing
E. Determine if employees have received a copy of or have easy access to agency security procedures and policies.	1. Inquire of appropriate personnel regarding employee access to agency security procedures and policies.
	2. Inspect evidence that employees have received a copy or have easy access to the agency security procedures and policies.
	3. Review policies and procedures in which employees have easy access to ensure that they are the most current.
F. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.	1. Identify all employees responsible for administering security.
	2. Review training records and certifications for all security employees to ensure that adequate training has been received.
	3. Inquire of appropriate personnel regarding the documentation and tracking of application specific training for employees.
	4. Review the most recent application specific training curriculum.
	5. Inspect evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked.
Section V: Review of periodic testing and evaluation of the effectiveness of IT security policies	
A. Determine if management reports for the review and testing of IT security policies and procedures, including network *RA*, accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	1. Inspect evidence that periodic testing of IT security policies and procedures (including network *RA*s, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted.
B. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspect evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
C. Determine if remedial action is being taken for issues noted on	1. Review policies and procedures for taking remedial action for issues noted on audits.

Control Activity	Detailed Testing
audits.	2. Inspect evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored.
Section VI: Review of Remedial Activities, processes, and reporting for deficiencies	
A. Determine if weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	1. Review policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness.
	2. Inspect evidence that weaknesses are tracked in a formal database (or other manner).
	3. Inspect evidence that planned actions to address all IT security weaknesses is being tracked.
B. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.	1. Review policies and procedures for preparing the CAP.
	2. Review all quarterly CAPs that were performed during the scope of the review to ensure that corrective actions have been taken to address IT security weaknesses.
C. Determine the number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.	1. Review policies and procedures for preparing CAPs.
	2. Review all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed.
	3. Inspect evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
Section VII: Review of Incident Detection, reporting, and response	
A. Determine that management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.	1. Review policies and procedures for monitoring systems and networks for unusual activity, and or intrusion attempts.
	2. Inspect evidence that management is monitoring systems and networks for unusual activity and/or intrusion attempts based on the policies and procedures.
B. Determine if management has procedures to take and has taken action in response to unusual activity, intrusion attempts and actual intrusions.	1. Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Inspect evidence that management has taken action in response to unusual activity, intrusion attempts, and/or actual intrusions if any have occurred within the scope of the review.
C. Determine that management processes and procedures include reporting of intrusion	1. Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.

Control Activity	Detailed Testing
attempts and intrusions in accordance with FISMA guidance.	2. Ensure that that policies and procedures are in accordance with FISMA standards.
Section VIII: Policies and procedures for continuity of operations and related physical security safeguards for IT systems.	
A. Determine if critical data and operations are formally identified and prioritized.	1. Review the Business Contingency Plan to ensure that critical data and operations are formally identified and prioritized.
B. Determine if resources supporting critical operations are identified in contingency plans.	1. Review the Business Contingency Plan to ensure that resources supporting critical operations are identified.
C. Determine if emergency processing priorities are established.	1. Review emergency processing priorities to ensure that they are formally documented.
D. Determine if data and program backup procedures have been implemented.	1. Review data and program backup policies and procedures.
	2. Inspect evidence (i.e., backup logs) that data and program backup procedures have been implemented.
E. Determine if adequate environmental controls have been implemented.	1. Inquire of data center manager concerning the environmental controls implemented in the data center.
	2. Perform Walkthrough of data center to ensure that adequate environmental controls have been implemented.
F. Determine if staff have been trained to respond to emergencies.	1. Review emergency response policies and procedures.
	2. Review emergency response training curriculum.
	3. Inspect evidence that emergency response training has been provided for applicable staff.
G. Determine that hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	1. Ensure that hardware maintenance procedures exist to help prevent unexpected interruptions.
	2. Ensure that problem management procedures exist to help prevent unexpected interruptions.
	3. Ensure that change management procedures exist to help prevent unexpected interruptions.
H. Determine if policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.	1. Review policies and procedures regarding the disposal of data and equipment to ensure that applicable Federal security and privacy requirements are included.

Control Activity	Detailed Testing
I. Determine if an up-to-date contingency plan is documented.	1. Inspect evidence that the contingency plan was approved within the scope of the review.
J. Determine if arrangements have been made for alternate data processing and telecommunications facilities.	1. Review the contingency plan to ensure that arrangements have been made for alternate data processing and telecommunications facilities.
	2. Review the contract with the organization that will provide alternate data processing and telecommunications operations if necessary.
K. Determine if the plan is periodically tested.	1. Review policies and procedures regarding periodically testing the contingency plan.
	2. Inspect evidence that the contingency plan has been periodically tested.
L. Determine if the results are analyzed and contingency plans adjusted accordingly.	1. Inspect evidence that the contingency plan is adjusted accordingly after the tests are performed and analyzed.
M. Determine if physical security controls exist to protect IT resources.	1. Inquire of data center manager concerning the physical security controls implemented in the data center.
	2. Perform Walkthrough of data center to ensure that adequate physical security controls exist.

Table D-4. Detailed SAS 70 Testing Procedures

Control Activity	Detailed Testing
A.1 An entity-wide security program has been documented, approved and monitored by management in accordance with the CMS Business Partners Systems Security Manual (BPSSM) and includes requirements to assess security risks periodically, establish a security management structure and clearly assign security responsibilities, implement effective security-related personnel policies, monitor the security program's effectiveness and ensure security officer training and employee security awareness.	
1. A security plan is documented and approved.	1. Reviewed the security plan. 2. Determined whether the plan covers the topics prescribed by OMB Circular A-130.
2. The security plan is kept current.	1. Reviewed the security plan and any related documentation indicating that it has been reviewed, updated and is current.
3. A security management structure has been established.	1. Reviewed the security plan and the entity's organization chart. 2. Interviewed security management staff. 3. Reviewed pertinent organization charts and job descriptions.
4. IS responsibilities are clearly assigned.	1. Reviewed the security plan. 2. Reviewed the security management's organization chart. 3. Reviewed the security management's formal job descriptions.
5. Owners and users are aware of security policies.	1. Reviewed documentation supporting or evaluating the awareness program. Observed a security briefing. 2. Interviewed data owners and system users. Determined what training they have received and if they are aware of their security-related responsibilities. 3. Reviewed memos, electronic mail files, or other policy distribution mechanisms. 4. Reviewed personnel files to test whether security awareness statements are current. 5. Called selected users, identified yourself as security or network staff, and attempted to talk them into revealing their password. 6. Reviewed security training schedules. 7. Reviewed security training materials. 8. For a selection of owners and users ensured that they have attended the required trainings.
6. Management periodically assesses the appropriateness of	1. Reviewed the reports resulting from recent assessments, including the most recent FMFIA

Control Activity	Detailed Testing
security policies and compliance with them.	report.
	2. Determined when last independent review or audit occurred and reviewed results.
	3. Reviewed written authorizations or accreditation statements.
	4. Reviewed documentation related to corrective actions.
	5. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	6. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
7. Employees have adequate training and expertise.	1. Reviewed job descriptions for security management personnel, and for a selection of other personnel.
	2. For a selection of employees, compared personnel records on education and experience with job descriptions.
	3. Reviewed training program documentation.
	4. Reviewed training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.
8. Employee training and professional development has been documented and formally monitored.	1. Inquired of the appropriate personnel regarding the documentation and formal monitoring of employee training and professional development.
	2. Reviewed policies and procedures regarding the documentation and formal monitoring of employee training and professional development.
	3. For a selected sample of employees, reviewed evidence that training and professional development is documented and formally monitored.
9. There is mandatory annual refresher training for security.	1. Reviewed policies and procedures regarding mandatory annual refresher security training
	2. Reviewed the most recent security awareness training curriculum.
	3. For a selected sample of employees, reviewed evidence that all attended the mandatory annual refresher security training.
10. Systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.	1. Reviewed policies and procedures regarding methods to make employees aware of security.
	2. Conducted a walk through of the site to ensure that posters/flyers are in fact hanging in visible areas.
	3. Inspected evidence that methods to make employees aware of security are implemented.

Control Activity	Detailed Testing
11. Employees have received a copy of or have easy access to agency security procedures and policies.	1. Inquired of appropriate personnel regarding employee access to agency security procedures and policies.
	2. Inspected evidence that employees have received a copy or have easy access to the agency security procedures and policies.
	3. Reviewed policies and procedures in which employees have easy access to ensure that they are the most current.
12. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.	1. Identified all employees responsible for administering security.
	2. Reviewed training records and certifications for all security employees to ensure that adequate training has been received.
	3. Inquired of appropriate personnel regarding the documentation and tracking of application specific training for employees.
	4. Reviewed the most recent application specific training curriculum.
	5. Inspected evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked.
A.2 Security related personnel policies are implemented that include performance of background investigations and contacting references, include confidentiality agreements with employees (regular, contractual and temporary) and include termination and transfer procedures that require exit interviews, return of property, such as keys and ID cards, notification to security management of terminations, removal of access to systems and escorting of terminated employees out of the facility.	
1. Hiring, transfer, termination, and performance policies address security.	1. Reviewed hiring policies and procedure to ensure that they address security.
	2. Reviewed transfer policies and procedures to ensure that they address security.
	3. Reviewed termination policies and procedures to ensure that they address security.
	4. Ensured that performance policies and procedures (i.e., *ROB* and Performance Evaluations) address security.
	5. Reviewed reinvestigation policies.
	6. Reviewed policies and procedures for performing background checks.
	7. For a selection of sensitive positions, inspected personnel records and determined whether background reinvestigations have been performed.
	8. Reviewed policies on confidentiality or security

Control Activity	Detailed Testing
	agreements.
	9. For a selection of such users, determined whether confidentiality or security agreements are on file.
	10. Reviewed vacation policies.
	11. Inspected personnel records to identify individuals who have not taken vacation or sick leave in the past year.
	12. Determined who performed vacationing employee's work during vacation.
	13. Reviewed job rotation policies.
	14. Reviewed staff assignment records and determined whether job and shift rotations occur.
	15. Reviewed pertinent policies and procedures.
	16. For a selection of terminated or transferred employees, examined documentation showing compliance with policies.
	17. Compared a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.
2. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
3. Employees have received a copy of the *ROB*.	1. Inquired of the appropriate personnel regarding the maintenance and distribution of the *ROB* for all types of employees.
	2. Reviewed the most current version of the *ROB*.
	3. Selected a sample of employees and ensured that they have received a copy of the most current version of the *ROB*.
A.3 Information resources are classified (risk-ranked) according to their criticality/sensitivity and are periodically formally reviewed.	
1. Resource classifications and related criteria have been established.	1. Reviewed data classification policies and procedures.
	2. Interviewed resource owners.
2. Owners have classified resources.	1. Reviewed resource classification documentation and compared to *RA*s. Discussed any discrepancies with appropriate officials.
3. Data sensitivity and integrity have been documented and data	1. Reviewed evidence based on policies and procedures that data has been classified.

Control Activity	Detailed Testing
has been classified.	
A.4 Access to computerized applications, systems software, and Medicare data is appropriately authorized, documented, and monitored, and includes approval by resource owners, procedures to control emergency and temporary access, and procedures to share and properly dispose of data.	
1. Resource owners have identified authorized users and their access authorized.	1. Reviewed pertinent written policies and procedures.
	2. For a selection of users (both application user and *IS* personnel) reviewed access authorization documentation.
	3. Interviewed owners and reviewed supporting documentation. Determined whether inappropriate access is removed in a timely manner.
	4. For a selection of users with dial-up access, reviewed authorization and justification.
	5. Interviewed security managers and reviewed documentation provided to them.
	6. Reviewed a selection of recent profile changes and activity logs.
	7. Obtained a list of recently terminated employees from Personnel and, for a selection, determined whether system access was promptly terminated.
2. Emergency and temporary access authorization is controlled.	1. Reviewed pertinent policies and procedures.
	2. Compared a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.
	3. Determined the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
3. Owners determine disposition and sharing of data.	1. Examined standard approval forms.
	2. Interviewed data owners.
	3. Examined documents authorizing file sharing and file sharing agreements.
4. Sanitation of equipment and media prior to disposal or reuse.	1. Reviewed written procedures.
	2. Interviewed personnel responsible for clearing equipment and media.
	3. For a selection of recently discarded or transferred items, examined documentation related to clearing of data and software.
	4. For selected items still in the entity's possession, tested that they have been appropriately sanitized.
5. Access authorizations are appropriately limited.	1. Reviewed policies and procedures regarding the disposal of data and equipment to ensure that

Control Activity	Detailed Testing
	applicable Federal security and privacy requirements are included.
	2. Interviewed management and systems personnel regarding access restrictions.
	3. Observed personnel accessing systems software, such as sensitive utilities, and noted the controls encountered to gain access.
	4. Attempted to access the operating system and other systems software.
	5. Selected some systems programmers and determined whether management-approved documentation supports their access to systems software.
	6. Selected some application programmers and determined whether they are not authorized access.
	7. Determined the last time the access capabilities of system programmers were reviewed.
6. Passwords, tokens, or other devices are used to identify and authenticate users.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security software password parameters.
	3. Observed users keying in passwords.
	4. Attempted to log on without a valid password; make repeated attempts to guess passwords.
	5. Assessed procedures for generating and communicating passwords to users.
	6. Reviewed a system-generated list of current passwords.
	7. Searched password file using audit software.
	8. Attempted to log on using common vendor supplied passwords.
	9. Interviewed users and security managers.
	10. Reviewed a list of IDs and passwords.
	11. Repeatedly attempted to log on using invalid passwords.
	12. Reviewed security logs.
	13. Reviewed pertinent policies and procedures.
	14. Reviewed documentation of such comparisons.
	15. Interviewed security managers.
	16. Made comparison using audit software.
	17. Viewed dump of password files (e.g., hexadecimal printout).
	18. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor obtained the assistance of a specialist.
7. Identification of access paths.	1. Reviewed access path diagram.

Control Activity	Detailed Testing
8. Logical controls over data files and software programs.	1. Interviewed security administrators and system users.
	2. Reviewed security software parameters.
	3. Observed terminals in use.
	4. Reviewed a system-generated list of inactive logon IDs, and determined why access for these users has not been terminated.
	5. Determined library names for sensitive or critical files and libraries and obtained security reports of related access rules. Using these reports, determined who has access to critical files and libraries and whether the access matches the level and type of access authorized.
	6. Performed penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system.
	7. When performing outsider tests, tested the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
	8. When performing insider tests, used an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, tried to access the entity's computer resources using default/generic IDs with easily guessed passwords.
	9. Determined whether naming conventions are used.
9. Logical controls over a database.	1. Reviewed pertinent policies and procedures.
	2. Interviewed database administrator.
	3. Reviewed DBMS and DD security parameters.
	4. Tested controls by attempting to access restricted files.
	5. Reviewed security system parameters.
10. Logical controls over telecommunications access.	1. Reviewed pertinent policies and procedures.
	2. Reviewed parameters set by communications software or teleprocessing monitors.
	3. Tested telecommunications controls by attempting to access various files through communications networks.
	4. Identified all dial-up lines through automatic dialer software routines and compared with known dial-up

Control Activity	Detailed Testing
	access. Discussed discrepancies with management.
	5. Interviewed telecommunications management staff and users.
	6. Reviewed pertinent policies and procedures.
	7. Viewed the opening screen seen by telecommunication system users.
	8. Reviewed the documentation showing changes to dial-in numbers.
	9. Reviewed entity's telephone directory to verify that the numbers are not listed.
11. Cryptographic tools.	1. To evaluate cryptographic tools, the auditor obtained the assistance of a specialist.
A.5 Security policies and procedures include controls to ensure the security of platform configurations and to ensure proper patch management of operating systems.	
1. All access paths have been identified and controls implemented to prevent or detect access for all paths.	1. Tested the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls.
	2. Obtained a list of vendor-supplied software and determined if any of these products have known deficiencies that adversely impact the operating system integrity controls.
	3. Judgmentally reviewed the installation of systems software components and determined whether they were appropriately installed to preclude adversely impacting operating system integrity controls.
	4. Performed an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods.
	5. Obtained a list of all systems software on test and production libraries used by the entity.
	6. Verified that access control software restricts access to systems software.
	7. Using security software reports, determined who has access to systems software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they *shall* be generated In the presence of the auditor.
	8. Verified that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
	9. Inquired whether disabling has occurred.

Control Activity	Detailed Testing
	10. Tested for default presence using vendor standard IDs and passwords.
	11. Determined what terminals are set up as master consoles and what controls exist over them.
	12. Tested to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.
2. Security policies and procedures include controls to address platform security configurations, and patch management.	1. Reviewed platform security configuration policies and procedures.
	2. Reviewed patch management policies and procedures.
3. Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
A.6 Physical access by all employees, including visitors, to Medicare facilities, data centers and systems is appropriately authorized, documented, and access violations are monitored and investigated.	
1. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	1. Reviewed a diagram of the physical layout of the computer, telecommunications, and cooling system facilities.
	2. Performed a walkthrough of data center to ensure that adequate physical security controls exist.
	3. Reviewed lists of individuals authorized access to sensitive areas and determined the appropriateness for access.
	4. Before becoming recognized as the auditor, attempted to access sensitive areas without escort or identification badges.
	5. Observed entries to and exits from facilities during and after normal business hours.
	6. Observed utilities access paths.
	7. Inquired of data center manager concerning the physical security controls implemented in the data center.
	8. Observed entries to and exits from sensitive areas during and after normal business hours.
	9. Reviewed procedures for the removal and return of storage media from and to the library.

Control Activity	Detailed Testing
	10. Selected from the log some returns and withdrawals, verified the physical existence of the tape or other media, and determined whether proper authorization was obtained for the movement.
	11. Observed practices for safeguarding keys and other devices.
	12. Reviewed written emergency procedures.
	13. Examined documentation supporting prior fire drills.
	14. Observed a fire drill.
2. Visitors are controlled.	1. Reviewed visitor entry logs.
	2. Observed entries to and exits from sensitive areas during and after normal business hours.
	3. Interviewed guards at facility entry.
	4. Reviewed documentation on and logs of entry code changes.
	5. Observed appointment and verification procedures for visitors.
3. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security violation reports.
	3. Examined documentation showing reviews of questionable activities.
4. Suspicious access activity is investigated and appropriate action is taken.	1. Tested a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.
	2. Interviewed senior management and personnel responsible for summarizing violations.
	3. Reviewed any supporting documentation.
5. Physical security controls exist to protect IT resources.	1. Inquired of data center manager concerning the physical security controls implemented in the data center.
	2. Performed walkthrough of data center to ensure that adequate physical security controls exist.
6. Physical and logical access controls have been established.	1. Interviewed management and subordinate personnel.
A.7 Medicare application and related systems software development and maintenance activities are authorized, documented, tested, and approved.	
1. Authorizations for software modifications are documented and maintained,	1. Identified recent software modifications and determined whether change request forms were used.
	2. Examined a selection of software change request forms for approvals.
	3. Interviewed software development staff.

Control Activity	Detailed Testing
2. Emergency changes are promptly tested and approved.	1. Reviewed procedures.
	2. For a selection of emergency changes recorded in the emergency change log, reviewed related documentation and approval.
3. Systems software changes are authorized, tested, and approved before implementation.	1. Reviewed pertinent policies and procedures.
	2. Interviewed management and systems personnel.
	3. Reviewed procedures for identifying and documenting systems software problems.
	4. Interviewed management and systems programmers.
	5. Reviewed the causes and frequency of any recurring systems software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.
	6. Determined what authorizations and documentation are required prior to initiating systems software changes.
	7. Selected recent systems software changes and determined whether the authorization was obtained and the change is supported by a change request document.
	8. Determined the procedures used to test and approve systems software prior to its implementation.
	9. Selected recent systems software changes were tested to verify indicated procedures were in fact used.
	10. Reviewed procedures used to control and approve emergency changes.
	11. Selected some emergency changes to systems software and tested whether the indicated procedures were in fact used.
4. Installation of systems software is documented and reviewed.	1. Interviewed management and systems programmers about scheduling and giving advance notices when systems software is installed.
	2. Reviewed recent installations and determine whether scheduling and advance notification did occur.
	3. Determined whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.
	4. Interviewed management, systems programmers, and library control personnel, and determined who migrates approved systems software to production libraries and whether outdated versions are removed from production libraries.

Control Activity	Detailed Testing
	5. Reviewed supporting documentation for some systems software migrations and the removal of outdated versions from production libraries.
	6. Interviewed data center management about their role in reviewing systems software installations.
	7. Reviewed some recent systems software installations and determined whether documentation shows that logging and management review occurred.
	8. Interviewed systems software personnel concerning a selection of systems software and determined the extent to which the operating version of the systems software is currently supported by the vendor.
	9. Interviewed management and systems programmers about the currency of systems software and the currency and completeness of software documentation.
	10. Reviewed documentation and tested whether recent changes are incorporated.
5. Management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	1. Reviewed the most current System Development Life Cycle.
	2. Reviewed additional information (i.e., *SSP*) which outline security controls included in the cost of developing new systems.
	3. Reviewed software change control policies and procedures to ensure that changes are being controlled effectively.
6. Management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	1. Performed inquiries of appropriate personnel regarding major systems maintained at the site.
	2. Reviewed documentation indicating accreditations and certifications were performed for the noted systems.
	3. Ensured that accreditations and certifications are in compliance with FISMA policies .
A.8 A System Development Life Cycle methodology is documented and in use and includes planning for and costs for security requirements in systems.	
1. A SDLC has been implemented.	1. Reviewed SDLC methodology.
	2. Reviewed system documentation to verify that SDLC methodology was followed.
	3. Interviewed staff.
	4. Reviewed training records.
2. Management activities include security controls in the costs of developing new systems as part	1. Reviewed additional information (i.e., *SSP*) which outline security controls included in the cost of developing new systems.

Control Activity	Detailed Testing
of their SDLC. Determine if procedures for software changes include steps to control the changes.	2. Reviewed software change control policies and procedures to ensure that changes are being controlled effectively.
3. Security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	1. Reviewed additional System Development Life Cycle policies and procedures to ensure that security polices and procedures have been incorporated.
	2. Performed inquiries of appropriate personnel regarding major systems maintained at the site.
	3. Reviewed documentation indicating accreditations and certifications were performed for the noted systems
A.9 Change management policies and procedures exist that include documented testing and approval of changes for regular and emergency changes and restrictions on the use of public domain and personal software.	
1. Authorizations for software modifications are documented and maintained.	1. Identified recent software modifications and determined whether change request forms were used.
	2. Examined a selection of software change request forms for approvals.
	3. Interviewed software development staff.
2. Use of public domain and personal software is restricted.	1. Reviewed pertinent policies and procedures.
	2. Interviewed users and data processing staff.
3. Changes are controlled as programs progress through testing to final approval.	1. Reviewed test plan standards.
	2. For the selected software change requests (1) reviewed specifications; (2) traced changes from code to design specifications; (3) reviewed test plans; (4) compared test documentation with related test plans; (5) analyzed test failures to determine if they indicate ineffective software testing; (6) reviewed test transactions and data*; (7) reviewed test results; (8) reviewed documentation of management or security administrator reviews; (9) verified user acceptance; and (10) reviewed updated documentation*.
	3. Determined whether operational systems experienced a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
4. Emergency processing priorities are established.	1. Reviewed emergency processing priorities to ensure that they are formally documented.
5. Data and program backup procedures have been implemented.	1. Reviewed data and program backup policies and procedures.
	2. Inspected evidence (i.e., backup logs) that data and

Control Activity	Detailed Testing
	program backup procedures have been implemented.
6. Hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	1. Reviewed hardware maintenance procedures that exist to help prevent unexpected interruptions.
	2. Reviewed problem management procedures that exist to help prevent unexpected interruptions.
	3. Reviewed change management procedures that exist to help prevent unexpected interruptions.
A.10 Access to program libraries is properly restricted and movement of programs among libraries is controlled.	
1. Programs are labeled and inventoried.	1. Reviewed pertinent policies and procedures.
	2. Interviewed personnel responsible for library control.
	3. Examined a selection of programs maintained in the library and assessed compliance with prescribed procedures.
	4. Determined how many prior versions of software modules are maintained.
2. Access to program libraries is restricted.	1. Examined libraries in use.
	2. Interviewed library control personnel.
	3. Verified that source code exists for a selection of production load modules.
	4. For critical software production programs, determined whether access control software rules are clearly defined.
	5. Tested access to program libraries by examining security system parameters.
	6. Selected some program tapes from the log and verified the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.
3. Movement of programs and data among libraries is controlled.	1. Reviewed pertinent policies and procedures.
	2. For a selection of program changes, examined related documentation to verify that: (1) procedures for authorizing movement among libraries were followed, and (2) before and after images were compared.
A.11 Adequate segregation of duties exists between various functions within Medicare operations and is supported by appropriately authorized and documented policies.	
1. Incompatible duties have been identified and policies implemented to segregate these duties.	1. Reviewed pertinent policies and procedures.
	2. Interviewed selected management and *IS* personnel regarding segregation of duties.
	3. Reviewed an agency organization chart showing *IS* functions and assigned personnel.

Control Activity	Detailed Testing
	4. Interviewed selected personnel and determined whether functions are appropriately segregated.
	5. Determined whether the chart is current and each function is staffed by different individuals.
	6. Reviewed relevant alternate or backup assignments and determined whether the proper segregation of duties is maintained.
	7. Observed activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	8. Reviewed the organizational chart and interviewed personnel to determine that assignments do not result in a single person being responsible for the indicated combination of functions.
	9. Determined through interview and observation whether data processing personnel and security managers are prohibited from these activities.
	10. Reviewed the adequacy of documented operating procedures for the data center.
2. Job descriptions have been documented.	1. Reviewed job descriptions for several positions in organizational units and for user security administrators.
	2. Determined whether duties are clearly described and prohibited activities are addressed.
	3. Reviewed the effective dates of the position descriptions and determined whether they are current.
	4. Compared these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	5. Reviewed job descriptions and interviewed management personnel.
3. Employees understand their duties and responsibilities.	1. Interviewed personnel filling positions for the selected job descriptions (see above). Determined if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	2. Determined from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	3. Interviewed management personnel in these

Control Activity	Detailed Testing
	activities.
4. Management reviews effectiveness of control techniques.	1. Interviewed management and subordinate personnel.
	2. Selected documents or actions that require supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).
	3. Determined which reviews are conducted to assess the adequacy of duty segregation. Obtained and reviewed results of such reviews.
5. Formal procedures guide personnel in performing their duties.	1. Reviewed manuals.
	2. Interviewed supervisors and personnel.
	3. Observed processing activities.
6. Active supervision and review are provided for all personnel.	1. Interviewed supervisors and personnel.
	2. Observed processing activities.
	3. Reviewed history log reports for signatures indicating supervisory review.
	4. Determined who is authorized to perform the *IPL* for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determined whether operators override the IPL parameters.
A.12 Activities of employees should be controlled via formal operating procedures that include monitoring of employee activities by management with documentation maintained to provide evidence of management's monitoring and review process.	
1. Audit trails are maintained.	1. Reviewed security software settings to identify types of activity logged.
2. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security violation reports.
	3. Examined documentation showing reviews of questionable activities.
3. Policies and techniques have been implemented for using and monitoring use of system utilities.	1. Reviewed pertinent policies and procedures.
	2. Interviewed management and systems personnel regarding their responsibilities.
	3. Determined whether logging occurs and what information is logged.
	4. Reviewed logs.
	5. Using security software reports, determined who can access the logging files.
4. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interviewed technical management regarding their reviews of privileged systems software and utilities usage.
	2. Reviewed documentation supporting their reviews.
	3. Interviewed management and systems personnel

Control Activity	Detailed Testing
	regarding these investigations.
	4. Reviewed documentation supporting these investigations.
	5. Interviewed systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Reviewed documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interviewed management and analyzed their reviews concerning the use of systems software.
	8. Determined what management reviews have been conducted, and their currency, over this area.
5. Formal procedures guide personnel in performing their duties.	1. Reviewed manuals.
	2. Interviewed supervisors and personnel.
	3. Observed processing activities.
6. Active supervision and review are provided for all personnel.	1. Interviewed supervisors and personnel.
	2. Observed processing activities.
	3. Reviewed history log reports for signatures indicating supervisory review.
A.13 A regular *RA* of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated annually. The assessment includes identification of threats, known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.	
1. Risks are periodically assessed.	1. Reviewed *RA* policies.
	2. Reviewed the most recent high-level *RA*.
	3. Reviewed the objectivity of personnel who performed and reviewed the assessment.
2. The current system configuration is documented, including links to other systems.	1. Reviewed the most recent system configuration.
	2. Reviewed the system configuration and/or related documentation indicating it has been reviewed and kept current.
3. Data sensitivity and integrity of the data have been documented and if data have been classified.	1. Reviewed data classification policies and procedures
	2. Reviewed evidence based on policies and procedures that data have been classified
4. Threat sources, both natural and manmade, have been formally identified.	1. Reviewed *RA* to ensure that threat sources, both natural and man-made, have been identified and documented.
5. A list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has	1. Reviewed the *RA* to ensure that a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed.

Control Activity	Detailed Testing
been developed and maintained current.	2. Reviewed the *RA* and/or related documentation indicating it has been reviewed and kept current.
6. An analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.	1. Reviewed the *RA* to ensure that mitigating controls are documented.
	2. Reviewed the *RA* to ensure that mitigating controls have been assessed and documented to determine if they adequately mitigate vulnerabilities.
7. Final risk determinations and related management approvals have been documented and maintained on file.	1. Reviewed the *RA* to ensure that final risk determinations are documented.
	2. Reviewed *RA* and/or related documentation indicating it has been approved (currently).
8. A mission/business impact analysis have been conducted and documented.	1. Reviewed documented critical business processes.
	2. Reviewed mission/business impact analysis to ensure that it has been documented for the critical business processes.
9. Obtain management's list of additional controls that have been identified to mitigate identified risks.	1. Reviewed any additional documented lists of controls identified to mitigate identified risks.
10. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.	1. Performed inquiries of appropriate personnel regarding systems for which controls have been tested.
	2. Reviewed evidence (i.e., internal/external audits) indicating system controls have been tested and evaluated for the identified systems.
	3. Reviewed evidence (i.e., internal/external penetration tests, etc) indicating system/network boundaries have been subjected to periodic reviews/audits.
	4. Ensured that all reviews have been performed within the scope of the review.
A.14 A centralized risk management focal point for IT *RA* has been established that includes promotion awareness programs, processes and procedures to mitigate risks, and monitoring processes to assess the effectiveness of risk mitigation programs.	
1. A security management structure has been established.	1. Reviewed the security plan and the entity's organization chart.
	2. Interviewed security management staff.
	3. Reviewed pertinent organization charts and job descriptions.
	4. Interviewed the security manager.
2. *IS* responsibilities are clearly assigned.	1. Reviewed the security plan.
3. Final risk determinations and related management approvals	1. Reviewed the *RA* to ensure that final risk determinations are documented.

Control Activity	Detailed Testing
have been documented and maintained on file.	2. Reviewed *RA* and/or related documentation indicating it has been approved (currently).
4. Obtain management's list of additional controls that have been identified to mitigate identified risks.	1. Reviewed any additional documented lists of controls identified to mitigate identified risks.
5. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	1. Reviewed the most current *RA*. 2. Reviewed IT Security policies and procedures to ensure that they reduce the risk outlined in the *RA*. 3. Ensured that IT Security policies and procedures are current.
6. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures. 2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
7. Management reports for the review and testing of IT security policies and procedures, including network *RA*, accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	1. Inspected evidence that periodic testing of IT security policies and procedures (including network *RA*s, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted.
8. Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
A.15 A *RA* and *SSP* has been documented, approved, and monitored by management in accordance with the CMS *IS* Risk Assessment and System Security Plan *Procedures*.	
1. Risks are periodically assessed.	1. Reviewed *RA* policies. 2. Reviewed the most recent high-level *RA*. 3. Reviewed the objectivity of personnel who performed and reviewed the assessment.

Control Activity	Detailed Testing
2. A security plan is documented and approved.	1. Reviewed the security plan.
	2. Determined whether the plan covers the topics prescribed by OMB Circular A-130.
3. The plan is kept current.	1. Reviewed the security plan and any related documentation indicating that it has been reviewed and updated and is current.
A.16 Regularly scheduled processes required to support the Medicare contractor's continuity of operations (data, facilities or equipment) are performed.	
1. Data and program backup procedures have been implemented.	1. Reviewed written policies and procedures for backing up files.
	2. Compared inventory records with the files maintained off-site and determined the age of these files.
	3. For a selection of critical files, located and examined the backup files. Verified that backup files can be used to recreate current reports.
	4. Determined whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.
	5. Located and examined documentation.
	6. Examined the backup storage site.
2. Adequate environmental controls have been implemented.	1. Examined the entity's facilities
	2. Interviewed site managers.
	3. Observed that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency.
	4. Observed the operation, location, maintenance and access to the air cooling system.
	5. Observed whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor.
	6. Determined whether the activation of heat and smoke detectors will notify the fire department.
3. Staff have been trained to respond to emergencies.	1. Interviewed data center staff.
	2. Reviewed training records.
	3. Reviewed training course documentation.
	4. Reviewed emergency response procedures.
	5. Reviewed test policies.
	6. Reviewed test documentation.
	7. Interviewed data center staff.
4. Effective hardware	1. Reviewed hardware maintenance procedures.

Control Activity	Detailed Testing
maintenance, problem management, and change management procedures exist.	2. Reviewed problem management procedures. 3. Reviewed change management procedures.
A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial action addressing findings noted from all security audits and reviews of IT systems, components and operations.	
1. Management ensures that corrective actions are effectively implemented.	1. Reviewed the status of prior-year audit recommendations and determined if implemented corrective actions have been tested. 2. Reviewed recent FMFIA reports. 3. Reviewed policies and procedures for ensuring that corrective actions are effectively implemented. 4. Reviewed evidence that management ensures that corrective actions are effectively implemented.
2. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.	1. Reviewed the most recent CMS CSR. 2. Noted GAPs in compliance as documented in the CMS CSR. 3. Reviewed management's response to the CSR to ensure that proper controls are in place/are in the process of being in place.
3. Weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	1. Reviewed policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness. 2. Inspected evidence that weaknesses are tracked in a formal database (or other manner). 3. Inspected evidence that planned actions to address all IT security weaknesses are being tracked.
4. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.	1. Reviewed policies and procedures for preparing CAPs. 2. Reviewed all quarterly CAPs that were performed during the scope of the review to ensure that corrective actions have been taken to address IT security weaknesses.
5. The number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.	1. Reviewed policies and procedures for preparing CAPs. 2. Reviewed all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed. 3. Inspected evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
6. Remedial action is being taken for issues noted on audits.	1. Reviewed policies and procedures for taking remedial action for issues noted on audits.

Control Activity	Detailed Testing
	2. Inspected evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored.
A.18 Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.	
1. An incident response capability has been implemented.	1. Interview security manager, response team members, and system users.
	2. Review documentation supporting incident handling activities.
	3. Determine qualifications of response team members.
2. Audit trails are maintained.	1. Review security software settings to identify types of activity logged.
A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts, and actual intrusions.	
1. Suspicious access activity is investigated and appropriate action is taken.	1. Reviewed polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Tested a selection of security violations to verify that follow-up investigations were performed, and to determine what actions were taken against the perpetrator.
	3. Interviewed senior management and personnel responsible for summarizing violations.
	4. Reviewed any supporting documentation.
	5. Reviewed policies and procedures and interviewed appropriate personnel.
	6. Reviewed any supporting documentation.
2. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interviewed technical management regarding their reviews of privileged systems software and utilities usage.
	2. Reviewed documentation supporting their reviews.
	3. Interviewed management and systems personnel regarding these investigations.
	4. Reviewed documentation supporting these investigations.
	5. Interviewed systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Reviewed documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interviewed management and analyzed their

Control Activity	Detailed Testing
	reviews concerning the use of systems software.
	8. Determined what management reviews have been conducted, and their currency, over this area.
A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with the Federal Information Security Management Act (FISMA)	
1. Management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	1. Reviewed polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Ensured that policies and procedures are in accordance with FISMA standards.

Appendix E:
CMS Guidelines

1 Introductory Comments to CMS Guidelines on Information Technology Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

1.1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This document provides introductory comments for a series of guidelines issued by the Centers for Medicare and Medicaid Services (CMS) to assist with the proper understanding and implementation of key security controls around CMS' data and information systems environment. The guidelines issued consist of the following:

1) Logical access controls and segregation of duties

2) Development and implementation of an entity-wide security plan

3) Application programmers' access to application data and source code and application programmer segregation of duties

4) Change management procedures and requirements for maintaining change management documentation

5) Testing process for the SANS Top 20 *Internet* Security *Vulnerabilities*

6) Implementation of security configuration templates

The intended audience of these guidelines, however, extends beyond CMS management and staff to include all CMS business partners.

Today's highly technology-dependent organization, while benefiting from the increased capabilities offered by continued improvements in Information Technology (IT), is also faced with the challenge of maintaining sufficient controls around the increased complexities of new developments in IT. The primary objectives of these controls are to maintain confidentiality, integrity, and availability around information critical to the organization's mission.

The six *(6)* guidelines mentioned above will provide CMS management and business partners with the information required to ensure that key *Federal* government recommended controls pertaining to each of the six topics are fully incorporated into CMS' current controls management environment.

1.2 Compliance Criteria

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The IT *controls* discussed in the guidelines are part of the foundation of operating in a secure environment promoting effective controls around data confidentiality, integrity, and availability. The importance of these controls is evidenced by the direct inclusion or indirect references to these controls in numerous *Federal* government Acts, standards, and guidelines, including, but not limited to, the following:

- Chief Financial Officers *(CFO)* Act of 1990
- Federal Financial Management Improvement Act (FFMIA) of 1996
- Federal Manager's Financial Integrity Act of 1982
- Federal Information Security Management Act *(FISMA)* of 2002
- Various *Office of Management and Budget (*OMB*)* circulars including OMB A-127 (Financial Management Systems) and OMB A-130 (Security of Federal Automated Information Resources)
- Various *National Institute of Standards and Technology (*NIST*)* Special Publications *(SP)* in the 800-series reports, and
- *General Accounting Office (*GAO*)*/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM)

The guidelines focus on the identification and description of controls pertaining to each of the six *(6)* control areas as recommended by FISCAM and FISMA (and other *Federal* government or industry standards, as required). Listed below is a brief discussion of the compliance framework for FISCAM and FISMA:

- A key goal of the *CFO* Act of 1990 was the development of a consistent approach to financial statement audits of *Federal* government agencies. *The* GAO Financial Audit Manual (FAM) provides detailed guidance on the performance of financial statement audits. In January of 1999, GAO issued the FISCAM as a companion to FAM. FISCAM provides the methodology for IT controls review within the framework of a financial statement audit of *Federal* government agencies.
- In February 2005, NIST published SP 800-53 *and in December 2007, NIST SP 800-53 Revision 2*to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002. According to the OMB memorandum titled "Memorandum for Heads of Executive Departments and Agencies", dated June 13, 2005, the *guidelines* documented in NIST SP 800-53 *(as amended) are* to be used by agencies *for selecting security controls for information systems supporting the executive agencies of the Federal government.*

The six *(6)* control areas discussed in the guidelines have manifested themselves within the management practices of CMS through the inclusion of a number of controls related to these areas in CMS' Business Partners Systems Security Manual (BPSSM). CMS has used OMB circulars, NIST Special Publication 800-series reports, and other *Federal* and industry guidelines to compile the IT management practices documented in BPSSM. Included in these practices are specific measures for the implementation of *C*ore *S*ecurity *R*equirements *(CSR)*. All controls listed in the BPSSM are mandatory for all *CMS* business partners. As such, the content of the BPSSM *shall* not be viewed as "guidance'. They are, rather, "requirements" for all CMS business partners.

1.3.1 Year-round Cyclical Approach

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Controls which are enforced through a periodic assessment against a static controls checklist will inevitably fail. Both the operations environment and the IT environment which supports it are fluid as are the security controls required to ensure data confidentiality, integrity, and availability. As such, the implementation of any control at CMS can only be effective if it is an integral part of the management process. This means incorporation of security controls in the year-round enterprise-wide management lifecycle of the organization.

FISCAM and NIST *SP* 800-53 *(as amended)* have each defined specific roles and responsibilities and an approach to planning and management of effective IT systems security. Within sections 2 and 3 of the BPSSM, CMS has also documented detailed descriptions of system security roles and responsibilities, and an approach to managing IT systems security.

CMS management is committed to ensuring that:

- Sections 2 and 3 of the BPSSM are continually evaluated against the IT security management approach and roles and responsibilities listed in FISCAM and NIST SP 800-53 to facilitate full compliance with these standards; and

- The BPSSM is continually evaluated for compliance with guidance in FISCAM and NIST SP 800-53 regarding specific systems to be covered by the security management program.

Table E-1 maps the key components of the IT security management approach recommended by FISCAM to those recommended by NIST *SP* 800-53 *(as amended)* and those required by BPSSM.

1.3.2 Management Involvement

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

As mentioned in the prior section, effective implementation of IT security controls can only be achieved if it is incorporated in the year-round enterprise-wide management lifecycle at the highest levels of an organization. This requires direct involvement, not only by the IT management structure (e.g., Chief Technology Officer and Chief Information Security Officer) but also by executives at the enterprise-wide level (e.g., program managers and agency leadership). This requirement is not only reflected in the compliance criteria used for the guidelines (e.g., the reporting requirements for FISMA) but also in other IT-related government publications and standards (e.g., the revised OMB Circular A-123, effective FY 2006).

Table E-1. Mapping of IT Security Program Management Principles

FISCAM	NIST 800-53	BPSSM (includes Chapter #)
Assess Risks & Determine Needs	Periodic risk assessments	3.10 Management Security Resources 3.2 Risk Assessment
Implement Policies and Controls	System security plans Policies and procedures based (on the risk assessments) and subordinate plans for providing adequate system security Plans and Procedures to Ensure Continuity of Operations for IT Systems	3.1 System Security Plan 3.4 IT Systems Contingency Plan 3.8 Fraud Control 3.9 Patch Management
Promote Awareness	Security awareness training	Attachment A Core Set of Security Requirements
Monitor & Evaluate Policy and Control Effectiveness	Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including: Network assessments Penetration activities Change management procedures Other Remedial activities, processes and reporting for deficiencies Incident detection, reporting, and response	3.3 Certification 3.5.1 Annual Compliance Audit 3.5.2 Plan of Action and Milestones 3.6 Incident Reporting and Response 3.7 System Security Profile

1.3.3 Reporting Requirements

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Given the fact that FISCAM's intended audience is financial statement auditors (i.e., Inspector Generals *(IG)* and independent auditors), it contains no reporting requirements directed specifically at agency management. FISMA however, contains specific reporting requirements for agency management as well as the *IG*.

According to the OMB Memorandum for Heads of Executive Departments and Agencies, published on June 13, 2005, regarding FISMA reporting instructions, "all agencies *shall* implement the requirements of FISMA and report annually to the *OMB* and Congress on the effectiveness of their security programs." According to the memorandum, each agency head's annual report *shall* be submitted to the Director of OMB and should comprise:

- A transmittal letter from the agency head, including a discussion of any differences between the findings of the agency *Chief Information Officer (*CIO*)* and IG
- Results of annual IT security reviews of systems and programs [completed by the CIO]
- Results of the IG's independent evaluation [completed by the IG]
- Status of agency compliance with OMB privacy policies [completed by the senior agency official for privacy]

The memorandum states that, prior to submission of the report, the CIO and IG assessment results need to be reconciled to resolve discrepancies, if any, between the two sections. *A* Plan of Action and Milestones (POA&M) *shall* be developed by each agency to correct weaknesses identified in the above reporting process. Reports documenting FISMA compliance updates *shall* be sent by the agency to OMB on a quarterly basis.

The memorandum emphasizes the fact that FISMA applies to information systems used or operated by an agency or by a contractor of the agency or other organization on behalf of the agency. It also states that agencies *shall* report both at an agency-wide level as well as by individual component. Clearly, the FISMA requirements apply to CMS *b*usiness *p*artners listed in the Introduction

In the CMS control environment, the BPSSM discusses a tool to *assist* CMS business partners conduct systems security *evaluation*. It is known as the *FISMA Evaluation (FE)* which is a module in the CMS Integrated Security Suite (CISS) tool. This module assists business partners to *perform their annual FISMA security control validation*. Upon completion of *the FE*, the business partner is required to submit the database to the CMS Central Office, the Consortium Contractor Management Officer and/or CMS Project Officer (CCMO/PO) [along with other required security documentation which is

described in section 3 of the BPSSM]. For CMS business partners, Joint Signature Memorandum JSM-05352, dated 05-17-05, specifies that POA&M reporting is to be performed on a monthly basis.

It is critical that the security review and reporting cycle prescribed by BPSSM follow a time table that allows for timely input to the FISMA reporting process and deadlines mentioned above.

1.4 Conclusion

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The primary objectives of effective IT controls are to maintain confidentiality, integrity, and availability *for* information critical to the organization's mission. Through the implementation of effective IT *c*ontrols security vulnerabilities can be reduced, security risks can be mitigated, and breaches in security can be identified and corrected in a timely manner. Examples of such security risks include theft and fraud. The implementation of the controls discussed in the six *(6)* guidelines, however, should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification, and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

2.1 Overview

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective IT controls is security and a key foundation of comprehensive security controls is **logical access controls and segregation of duties**. This guideline *shall*:

- Provide a high level understanding of **logical access controls and segregation of duties**,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related to **logical access controls and segregation of duties**, and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

2.2 Introduction to Logical Access Controls and Segregation of Duties

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The BPSSM defines access controls *as "the process of granting or denying specific requests to: (i) obtain and use information and related information processing services; and (ii) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances)."*

According to FISCAM, key objectives of logical access controls are to ensure that: (1) users have only the access needed to perform their duties, (2) access to very sensitive resources, such as security software programs, is limited to very few individuals, and (3) employees are restricted from performing incompatible functions or functions beyond their responsibility.

FISCAM states that "If these objectives are met, the risk of inappropriate modification or disclosure of data can be reduced without interfering with the practical needs of users. However, establishing the appropriate balance between user needs and security requires a careful analysis of the criticality and sensitivity of information resources available and the tasks performed by users."

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers (IDs), passwords, or other identifiers that are linked to predetermined access privileges. Controls should be designed to restrict legitimate users to the specific systems, programs, and files needed to perform their duties while inhibiting access by others.

FISCAM defines "segregation of duties" as controls that describe how work responsibilities should be segregated so that one person does not have access to or control

over all of the critical stages of an information handling process. For instance; while representatives of the user community may initiate requests for changes to system capabilities, computer programmers should not be allowed to write, test, and approve program changes; and a user who has entered transactions in the system, should not have the capability to also review and approve the processing of all such transactions. Often, proper segregation of duties is achieved by splitting responsibilities between two or more organizational groups to ensure independence and objective checks and balances. Controls can be enforced through automated and/or manual measures.

2.3 Risks of Non-compliance

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Per FISCAM, "inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure and modification of data". Following are examples, extracted from FISCAM, which illustrate the potential consequences of such vulnerabilities.

- By obtaining direct access to **data files**, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could: (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) inadvertently or purposefully change a receivable balance, or (4) obtain confidential information about business transactions or individuals.

- By obtaining access to **application programs** used to process transactions, an individual could make unauthorized changes to these programs or introduce malicious programs, which in turn could be used to access data files, resulting in situations similar to those describe above, or to process unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for himself or herself.

- By obtaining access to **computer facilities and equipment**, an individual could: (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.

FISCAM states that "inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed." FISCAM provides the following examples of potential consequences of inadequate controls around segregation of duties:

- *An* individual who was independently responsible for authorizing processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or

- *A* computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Within appendix C of the BPSSM, CMS outlines a number of specific safeguards against employee fraud. **Segregation of duties** is listed as a key safeguard against employee fraud. For a more detailed look into each of the measures for the prevention and detection of fraudulent activities see appendix C of the BPSSM.

2.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place which satisfy the control objective.**

Table E-3 and Table E-4 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to **logical access controls and segregation of duties**. Refer to Chapter 3 of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-3. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-4.

The FISMA compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare claims processing systems and Medicare data center systems be categorized as "high impact" security systems.

As mentioned above, Table E-4 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to **logical access controls and segregation of duties**. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-4 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-4, the corresponding FISCAM control in Table E-3, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) include the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with **logical access controls and segregation of duties** guidelines.

2.5 Sample Instances of Non-Compliance and Recommended Resolution

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Table E-2 below provides a listing of sample instances of non-compliance with logical access controls and segregation of duties based on prior controls reviews and audits. Specifically, the table lists the findings, issues and recommended course of action for selected cases of non-compliance. The findings and issues in this table are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings and issues have been selected instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue takes into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the table for a specific issue may not apply to all sites.

Table E-2. Sample Findings from Prior CMS Controls Reviews and Audits

Finding	Issue	Suggested Remediation
Password management controls need to be strengthened	1. Some user accounts were not set to force the use of a combination of alphabetical, numeric, and/or special characters.	Force RACF password configuration settings to include a combination of alphabetical, numeric, and/or special characters (may require an exit).

Finding	Issue	Suggested Remediation
	2. Management does not have a process for periodically reviewing user ID profiles to ensure that these profiles are not configured with inappropriate settings.	Periodically review user accounts and passwords to ensure that they adhere to BPSSM requirements and applicable FISCAM Controls and Control Techniques, e.g., access settings reflect job responsibilities, use of alpha-numeric passwords, etc. These controls can be enforced through, manual as well as automated, means.
Logical access controls need to be strengthened	1. Revoked RACF user IDs are not being promptly removed from the mainframe system.	Clarify and document the programs, processes, and procedures used to periodically review and remove "revoked" user IDs from the system. Document and maintain justifications for revoked RACF user IDs on the system, as well as, authorizations for the reactivation or deletion of these accounts.
	2. Access to the DB2 system, which contains sensitive Medicare information, is not being restricted to users on a "need to know" basis.	Update the database administration policies and procedures to include comprehensive processes and procedures regarding the maintenance of documented RACF user authorizations to access DB2 data sets containing sensitive Medicare data. Document and maintain authorizations for all RACF user IDs with access to DB2 data sets containing sensitive Medicare data. Develop, document, and implement processes and procedures to monitor user accesses to sensitive Medicare data maintained in DB2 data sets and to take appropriate action when questionable access is detected.
Resource owners have not identified or granted access to authorized users.	1. No user access documentation exists for network devices, including the Cisco router and the Cisco PIX firewall.	Continue efforts in developing a logging and monitoring strategy for Cisco routers and Cisco PIX firewalls. The strategy should be implemented on the Medicare systems and throughout the organization. A policy should also be developed to outline roles and responsibilities in ensuring that the systems are configured correctly and that logs are being generated and reviewed. A formal user access policy should be complied with for granting users access to all network devices including Cisco routers and Cisco PIX firewalls.
	2. Access to the Cisco routers and the Cisco PIX firewall are not proactively monitored.	
	3. Logging is disabled on the Cisco PIX firewall.	

Finding	Issue	Suggested Remediation
Oracle database control deficiencies	1. A process for establishing the accounts is not defined and documented.	Develop and document procedures for establishing Oracle accounts.
	2. The defined privileges are not periodically assessed and revalidated.	Develop and document procedures for reviewing Oracle accounts, account privileges, and user roles.
	3. Procedures for assigning user roles have not been documented.	Develop and document procedures for assigning user roles.
	4. Oracle logs are not reviewed and automated tools to assist in log reviews do not exist.	Develop and document procedures for reviewing Oracle logs. Research and implement automated tools to assist in log reviews and monitoring.
	5. The configuration setting to provide log actions performed by privileged accounts was not set.	Configure the Oracle initialization file to generate audit logs of actions performed by privileged users.
Improvements in Password controls over network devices that allow Dial-in access	1. Noted poor password controls for devices that allow access to the network. As a result, passwords could be easily guessed.	Management should establish, implement, and enforce formal policies and procedures for remote access password-use ensuring that "hard-to-guess" passwords are required for authentication of remote users.
Password Parameters did not meet CMS Core Security Requirements	For the mainframe, the following ACF2 password settings were used:	ACF2 policies should be improved to meet the minimum requirements outlined in the CMS Core Security Requirements. Correct and resubmit CMS CAST worksheets to reflect the current environment.
	1. PSWD HISTORY = NO - Activates default history of one generation. Old passwords may be used after one generation	
	2. MIN PSWD LENGTH = 5 - Allowed five characters for a minimum.	

Finding	Issue	Suggested Remediation
	3. LOGON RETRY COUNT = 3 - Does not deactivate the user ID after three failed passwords, but rather logs the terminal session off. The user can immediately restart the session and conduct additional logon attempts.	
	4. MAX PSWD ATTEMPTS = 6 - Allows a user ID to have six invalid password attempts during a password change period, at which time the account is locked out.	
Job rotation and vacation policy does not exist	A formal policy mandating periodic job rotations and vacation for personnel does not exist.	We recommend that management incorporate a formal job rotation and vacation policy so that responsibilities can be re-assigned to different individuals. Should neither of the above two measures exist, we recommend the monitoring of employee activities who are exposed to sensitive data over extended periods in order to reduce potential security risks.

2.6 Periodic Review and Testing of Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems, and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

3.1 Overview

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is the **development and implementation of an entity-wide security plan.** This guideline *shall*:

- Provide a high level understanding of the **development and implementation of an entity-wide security plan,**
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related to the **development and implementation of an entity-wide security plan,** and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

3.2 Introduction to the Development and Implementation of an Entity-wide Security Plan

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Business Partners Systems Security Manual (BPSSM) defines entity-wide security plan controls as controls that "address the planning and management of an entity's control structure."

According to GAO FISCAM, key objectives of entity-wide security program planning and management are to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer related controls.

FISCAM states that "An entity-wide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures."

Comprehensive guidance on planning and managing an entity-wide security plan is contained in FISCAM Appendix VIII, titled "Principles for managing an information security program."

3.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-3 and E-4 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to the **development and implementation of an entity-wide security plan**. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-3. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-4.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-4 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to the development and implementation of an entity-wide security plan. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-7 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-7, the corresponding FISCAM control in Table E-6, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores

Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) include the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines around the **development and implementation of an entity-wide security plan.**

3.6 Periodic Review and Testing of Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

4.1 Overview

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is controls around **access for application programmers to application data and source code.**

This guideline *shall*:

- Provide a high level understanding of controls around **access for application programmers to application data and source code,**

- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which directly concern **access for application programmers to application data and source code,** and

- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

4.2 Introduction to Access Controls for Application Programmers to Application Data and Source Code

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Business Partners Systems Security Manual (BPSSM) defines application software development and change controls as controls that "address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information."

The GAO FISCAM states that "Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled."

A key component of comprehensive access controls for application programmers is 'Segregation of Duties'. FISCAM defines 'Segregation of duties' as controls that describe how work responsibilities should be segregated so that one person does not have access to or control over all of the critical stages of an information handling process. For instance; while a representative of the user community may initiate requests to changes in system capabilities, computer programmers should not be able to write, test, and approve program changes; and a user who has entered transactions in the system, should not have the capability to also review and approve the processing of all such transactions. Often, proper segregation of duties is achieved by splitting responsibilities between two or more

organizational groups to ensure independence and objective checks and balances. These controls can be enforced through automated and/or manual measures.

4.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-9 and E-10 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to **application programmers' access to application data and source code**. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-9. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-10.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-10 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to **application programmers' access to application data and source cod**e. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-10 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-10, the corresponding FISCAM control in Table E-9, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines **around application programmers' access to application data and source code.**

4.6 Periodic Review and Testing of Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

5.1 Overview

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is **change management procedures.** Included in the controls around change management are requirements for maintaining change management documentation.

This guideline *shall*:

- Provide a high level understanding of **change management procedures**,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related **change management procedures,** and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

5.2 Introduction to Change Management Procedures

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Business Partners Systems Security Manual (BPSSM) defines application software development and change controls as controls that "address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information."

The GAO FISCAM states that:

> "Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled."
>
> "Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally, the application users have the primary responsibility for authorizing systems changes. However, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective. For this reason, an entity may require a senior systems developer to co-authorize a change."
>
> "The use of standardized change request forms helps ensure that requests are clearly communicated and that all approvals are documented. Authorization documentation should be maintained for at least as long as a system is in

operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected."

5.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-12 and E-13 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to change management procedures. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-12. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-13.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-13 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to **change management procedures.** Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-13 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-13, the corresponding FISCAM control in Table E-12, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines around **change management procedures.**

5.6 Periodic Review and Testing of Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

6.1 Overview

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is the **implementation and maintenance of security configuration templates.**

This guideline *shall*:

- Provide a high level understanding of **implementation and maintenance of security configuration templates,**
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related to the **implementation and maintenance of security configuration templates,** and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

6.2 Introduction to the Implementation and Maintenance of Security Configuration Templates

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Business Partners Systems Security Manual (BPSSM) and the GAO FISCAM define configuration management as "the control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system."

The BPSSM also states "The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires NIST to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal *g*overnment. The guidelines and checklists are developed to help system operators configure security within these systems to the highest level possible."

NIST has produced Special Publication 800-70 "Security Configuration Checklists Program for IT Products - Guidance for Checklist Users and Developers" to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products.

NIST also states that "a security configuration checklist" (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular operational environment. It could also include templates or automated scripts and other procedures. Checklists can be created by IT vendors for their own products or created by other organizations such as consortia,

academia, open source, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products."

6.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Security configuration templates take one of two forms. Some configuration templates are software-based in the form of a file or files which contain predetermined security settings which can be applied to single or multiple systems in an automated fashion. The other type of configuration template is policy-based and in the form of a checklist or recommendations guide, applied manually to the system during initial build and deployment.

Both NIST and the NSA provide security configuration checklists and security configuration guides for multiple operating systems and applications. Additionally, Security Technical Implementation Guides (STIGs) are published as tools to assist in the improvement of the security of Department of Defense (DOD) information systems. They are created using the principle that the most effective way to improve security in information systems is to include security in the initial design and development. As such, they provide the technical security policies, requirements, and implementation details for applying security concepts to information systems.

According to the BPSSM, CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program. Specifically, MACs and EDCs are required to start with these baseline configurations listed in the Security Technical Implementation Guides (STIGs) and document any exceptions based on environment-specific implementation. The use of STIGs *shall*:

- Reduce the likelihood of successful intrusions or attacks;
- Facilitate secure configuration of systems prior to network deployment;
- Assist with monitoring systems for on-going conformance with security configurations

Section 3.10.1 of this document (BPSSM) contains a list of applicable STIGs and their location.

Some operating system vendors include robust configuration management capabilities within the software. For example, Microsoft has included multiple methods to natively manage the configuration of Windows systems. The Windows Security Configuration Manager tool set allows administrators to create, apply and edit the security for local computers, organizational units, or domains. Windows also allows the construction and application of software-based security configuration templates. Microsoft states,

"With the Security Templates snap-in for Microsoft Management Console, administrators can create a security policy for computers or for networks. It is a single point of entry where the full range of system security can be taken into account. The Security Templates snap-in does not introduce new security parameters; it simply organizes all existing security attributes into one place to ease security administration."

The BPSSM states that "Business partners are **required** to perform an annual risk assessment in accordance with the CMS Information Security RA Methodology." The relevant FISCAM and NIST SP 800-53 controls identified to mitigate the risks discovered in the risk assessment can then be used to develop effective security configuration templates. Additionally, the BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-15 and E-16 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to the **implementation and maintenance of security configuration templates**. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-15. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-16.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-16 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to the **implementation and maintenance of security configuration templates**. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for “supplemental guidance” on each control listed in Table E-16 and to Appendix E of NIST SP 800-53 for a description of “Minimum Assurance Requirements” for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-16, the corresponding FISCAM control in Table E-15, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on “control techniques” and “audit procedures” for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines related to the **implementation and maintenance of security configuration templates**.

6.6 Periodic Review and Testing of Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems (which all CMS systems are

considered to be). Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls. Additionally, the BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

FISCAM refers to the maintenance of security configuration templates more specifically when it discusses maintaining System Security Plans. It states,

> "To be effective, the policies and plan should be maintained to reflect current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the types and configuration of computer resources in use. Revisions to the plan should be reviewed, approved, and communicated to all employees. Outdated policies and plans not only reflect a lack of top management concern, but also may not address current risks and, therefore, may be ineffective."

The BPSSM states that "CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity." As requirements change or arise from the configuration management program, these new changes should be reflected by changes in the appropriate template.

7.1 Overview

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls includes a **Testing Process for the SANS Top 20 Internet Security Vulnerabilities**. This guideline *shall*:

- Provide a high level understanding of the SANS Top 20 Internet Security Vulnerabilities,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related to Testing for the SANS Top 20 Internet Security Vulnerabilities, and
- Provide a sample of prior instances of lack of identification and remediation of the SANS Top 20 Internet Security Vulnerabilities and recommended testing approaches.

7.2 Introduction to Testing for the SANS Top 20 Internet Security Vulnerabilities

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The GAO FISCAM states that an important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. To implement an effective security plan, top management should monitor its implementation and adjust the plan in accordance with changing risk factors. Over time, policies and procedures may become inadequate because of changes in operations or deterioration in the degree of compliance. Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan.

OMB Circular A-130, Appendix III, requires that *Federal* agencies review the security of their general support systems and major applications at least once every 3 years or sooner, if significant modifications have occurred or where the risk and magnitude of harm are high.

In addition, the Federal Managers Financial Integrity Act (FMFIA) of 1982 and OMB Circular A-123 require agencies to annually assess their internal controls, including computer-related controls, and report any identified material weaknesses to the President and the Congress.

When significant weaknesses are identified, the related risks should be reassessed, appropriate corrective actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. This is an important aspect of management's risk management responsibilities. In addition to modifying written policies to correct

identified problems, implementation of the corrective actions should be tested to see whether they are understood and are effective in addressing the problem. Management should continue to periodically review and test such corrective actions to see that they remain effective on a continuing basis.

The SANS (SysAdmin, Audit, Network, Security) Institute (or simply SANS) is one of the most trusted and largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center. SANS was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community.

The "Top Ten" list was first released by the SANS Institute and the National Infrastructure Protection Center (NIPC) in 2000. Today, though it is now called the Top Twenty, it covers over 230 well-known, often-exploited vulnerabilities in the Windows and UNIX environments. Thousands of organizations use the list to prioritize their efforts so they can close the most dangerous holes first. The majority of successful attacks on computer systems via the Internet can be traced to the exploitation of security flaws on this list. The SANS/FBI Top Twenty includes step-by-step instructions and pointers to additional information useful for correcting the flaws. SANS updates the list and the instructions as more critical threats and more current or convenient methods are identified.

The SANS Institute states that the SANS Top-20 2004 is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited elements in UNIX (SUN Solaris, IBM AIX, HP-UX, BSD, and Linux, etc.) environments. There are thousands of security incidents each year affecting these operating systems; however, the overwhelming majority of successful attacks target one or more of these twenty vulnerable services.

7.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The SANS Top-20 list is a living document and is regularly updated. It includes step-by-step instructions and pointers to additional information useful for correcting common security flaws in Windows and UNIX operating systems. SANS updates the list and the instructions as more critical threats and more current or convenient methods of protection are identified. Table E-18 provides a list of the 20 vulnerable as described by the SANS Institution.

Table E-17. SANS Top 20 Internet Security Vulnerabilities (as of 10/08/04 – v. 5)

Top Vulnerabilities to Windows Systems
W1 - Web Servers & Services
W2 - Workstation Service
W3 - Windows Remote Access Services
W4 - Microsoft SQL Server (MSSQL)
W5 - Windows Authentication
W6 - Web Browsers
W7 - File-Sharing Applications
W8 - LSAS Exposures
W9 - Mail Client
W10 - Instant Messaging
Top Vulnerabilities to UNIX Systems
U1 - BIND Domain Name Service (DNS)
U2 - Web Server
U3 - Authentication
U4 - Version Control Systems
U5 - Mail Transport Service
U6 - Simple Network Management Protocol (SNMP)
U7 - Open Secure Sockets Layer (SSL)
U8 - Misconfiguration of Enterprise Services NIS/NFS
U9 - Databases
U10 - Kernel

For each of the vulnerabilities, SANS lists on its website: description, operating system affected, related CVE entries, how to protect against the vulnerability, and how to test to determine if the vulnerability exists on a system. For the testing process for each vulnerability SANS indicates the manual process for testing (if any) as well as examples of automated tools (both open source and commercial) which can scan for the vulnerability.

NIST Special Publication 800-42, Guideline on Network Security Testing, identifies several different types of security testing and vulnerability monitoring. Some testing techniques are predominantly manual, requiring an individual to initiate and conduct the test. Other tests are highly automated and require less human involvement. Regardless of the type of testing, staff that setup and conduct security testing should have significant security and networking knowledge, including significant expertise in the following areas: network security, firewalls, intrusion detection systems, operating systems, programming and networking protocols (such as TCP/IP).

The following are types of testing techniques and tools:

- Network Scanning
- Vulnerability Scanning
- Password Cracking
- Log Review
- Integrity Checkers
- Virus Detection
- War Dialing
- War Driving (802.11 or wireless LAN testing)
- Penetration Testing

NIST SP 800-42 also references the SANS Top 20 Internet Security Vulnerabilities in its discussion and recommendations regarding security testing. NIST specifically states that the main focus of this document is the basic information about techniques and tools for individuals to begin a network security testing program. But it also states that this document is by no means all-inclusive. Individuals and organizations should consult the references provided in this document, such as the SANS list, as well as vendor product descriptions and other sources of information. And although the document is not all-inclusive, it is comprehensive in that it discusses how to implement security testing for vulnerabilities such as the SANS list while keeping a perspective of aligning with other security related practices for government information systems (such as the System Development Life Cycle and Certification and Accreditation processes).

The BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-19 and E-20 list the controls in FISCAM and NIST SP 800-53 respectively which are applicable to **a Testing Process for the SANS Top 20 Internet Security Vulnerabilities**. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-19. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-20.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims

Processing Systems and Medicare Data Center systems be categorized as “high impact” security systems.

As mentioned above, Table E-20 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to **Testing for the SANS Top 20 Internet Security Vulnerabilities**. Refer to NIST SP 800-53 for a description of each control and the applicable “Control Enhancements” for “High Control Baseline” (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for “supplemental guidance” on each control listed in Table E-20 and to Appendix E of NIST SP 800-53 for a description of “Minimum Assurance Requirements” for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-20, the corresponding FISCAM control in Table E-19, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on “control techniques” and “audit procedures” for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines related to **Testing for the SANS Top 20 Internet Security Vulnerabilities.**

7.6 Periodic Review and Testing of Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict

adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems (which all CMS systems are considered to be). Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

Often, several of these testing techniques are used together to gain a more comprehensive assessment of the overall network security posture. For example, penetration testing usually includes network scanning and vulnerability scanning to identify vulnerable hosts and services that may be targeted for later penetration. Some vulnerability scanners incorporate password cracking. None of these tests by themselves will provide a complete picture of the network or its security posture.

NIST Special Publication 800-42 Guideline on Network Security Testing stresses the need for an effective security testing program within *Federal* agencies. Testing serves several purposes. One, no matter how well a given system may have been developed, the nature of today's complex systems with large volumes of code, complex internal interactions, interoperability with uncertain external components, unknown interdependencies coupled with vendor cost and schedule pressures, means that exploitable flaws will always be present or surface over time. Accordingly, security testing must fill the gap between the state of the art in system development and actual operation of these systems. Two, security testing is important for understanding, calibrating, and documenting the operational security posture of an organization. Aside from development of these systems, the operational and security demands must be met in a fast changing threat and vulnerability environment. Attempting to learn and repair the state of your security during a major attack is very expensive in cost and reputation, and is largely ineffective. Three, security testing is an essential component of improving the security posture of organizations. Organizations that have an organized, systematic, comprehensive, ongoing, and priority driven security testing regimen are in a much better position to make prudent investments to enhance the security posture of their systems.

The BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

8 References

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999.

OMB Guidance on FISMA Reporting Instructions, Memorandum for Heads of Executive Departments and Agencies, June 13, 2005.

Federal Information Security Management Act (FISMA) of 2002.

NIST Special Publication 800-53 *Revision 2*, Recommended Security Controls for Federal Information Systems, *December 2007*.

Appendix F:
Security Configuration Management

Table of Contents

(Rev. 9, 06-20-08)

1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires *the National Institute of Standards and Technology (*NIST*)* to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal *government*.

2 Security Technical implementation Guides (STIG)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The guidelines, called STIG*s*, and checklists, called Security Checklists, are developed to help system operators configure security within their systems to the highest level possible. The STIGs and Security Checklists were formerly available at a NIST web page because the source Defense Information Systems Agency (DISA) web page was restricted to users in .gov and .mil domains. That restriction is no longer in effect, so NIST no longer hosts the DISA STIG and Security Checklist links.

The DISA *Web* page link for STIGs is: *http://iase.disa.mil/stigs/stig/index.html*, and for Security Checklists: *http://iase.disa.mil/stigs/checklist/index.html*. CMS recommends that business partner *Systems Security Officers (*SSO*)* (or their designated representative) subscribe to the DISA STIG-News Mailing List at: *http://iase.disa.mil/stigs/index.html* so they will be notified whenever updated or new STIGs become available.

The National Security Agency (NSA) has also developed and distributed configuration guidance for a wide variety of software from open-source to proprietary. The objective of the NSA configuration guidance program is to provide administrators with the best possible security options in the most widely used products. NSA provides these guidelines at: *http://www.nsa.gov/snac/downloads_all.cfm*.

The Center for Internet Security (CIS) provides security configuration benchmarks that represent a prudent level of due care, and are working to define consensus best-practice security configurations for computers connected to the Internet. CIS scoring tools analyze and report system compliance with the technical control settings in the benchmarks. The CIS benchmarks and scoring tools are available for download at: *http://www.cisecurity.com/benchmarks.html*.

The use of STIGs:

- Reduce*s* the likelihood of successful intrusions or attacks;
- Facilitate*s* secure configuration of systems prior to network deployment; and
- Assist*s* with monitoring systems for on-going conformance with security configurations.

The latest versions of these documents can be obtained from the DISA web site by subscribing to the STIG-News Mailing List to receive update notifications.

3 Department of Health and Human Services Minimum Security Configuration Standards

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Department of Health and Human Services (*D*HHS) is responsible for implementing and administering an information assurance and privacy program to protect its information resources, in compliance with applicable public laws, *F*ederal regulations, and Executive Orders, including the Federal Information Security Management Act of 2002 (FISMA); the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, dated November 28, 2000; and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The *D*HHS Minimum Security Configuration Standards were created as part of the *D*HHS Information Assurance and Privacy Program to supply standards for configuring Departmental Systems and Applications using Minimum Standard Configurations.

At a minimum, CMS expects *business partners to comply* with the *D*HHS configuration standards described below.

4 DHHS Federal Desktop Core Configuration (FDCC) Standard for Windows XP

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The DHHS is responsible for implementing and administering an information security and privacy program to protect its information resources. The DHHS must be compliant with applicable public laws, Federal regulations, and Executive Orders, including

FISMA; OMB Circular A-130, Management of Federal Information Resources, and HIPAA. To meet these requirements, DHHS instituted the DHHS Information Security Program Policy and the DHHS Information Security Program Handbook documents.

The DHHS developed the DHHS Federal Desktop Core Configuration (FDCC) Standard for Windows XP in response to OMB Memorandum (M)-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems, released on March 22, 2007. In collaboration with its Operating Divisions (OPDIVs), DHHS developed the standard by testing the original FDCC standard provided by NIST on July 31, 2007, and making appropriate adjustments to best suit the DHHS and its OPDIV's environment. The resulting DHHS FDCC Standard must be implemented at each OPDIV (i.e., CMS) and its contractor computers that are owned or operated by a contractor on behalf of, or for, the OPDIV, or are integrated into a Federal system subject to FDCC.

The DHHS considers the DHHS FDCC Standard for Windows XP document "sensitive" so it is not publicly available. To obtain a copy of the DHHS FDCC Standard, the designated Systems Security Officer (SSO) from each business partner must request a copy via the CISS Help Desk (CISS@ngc.com). CMS expects business partners to request a copy and comply with the DHHS FDCC Standard for Windows XP.

Appendix G:
Acronyms and Abbreviations

(Rev. 9, 06-20-08)

A

AAL	*Authorized Access List*
ABMAC	*A/B Medicare Administrative Contractor*
AC	*Access Control*
ACA	*Annual Compliance Audit*
ADM	*Administrative*
ADP	*Automated Data Processing*
AFE	*Annual Frequency Estimate*
AIE	*Annual Impact Estimate*
AIS	*Automated Information System*
AISSP	*Automated Information Systems Security Program*
ALE	*Annual Loss Expectancy*
ANSI	*American National Standards Institute*
APF	*Authorized Program Facility*
ARO	*Annualized Rate of Occurrence*
ARS	*Acceptable Risk Safeguards*
ASC	*Accredited Standards Committee*
AT	*Awareness and Training*
AU	*Audit and Accountability*

C

C&A	*Certification and Accreditation*
CA	*Certification, Accreditation, and Security Assessments*
CAP	*Corrective Action Plan*
CAST	*Contractor Assessment Security Tool*
CCMO	*Consortium Contractor Management Officer*
CD	*Compact Disc*
CD-ROM	*Compact Disc-Read Only Memory*
CFO	*Chief Financial Officer*
CFR	*Code of Federal Regulations*
CIA	*Confidentiality, Integrity, Availability*
CICG	*Critical Infrastructure Coordination Group*
CIO	*Chief Information Officer*
CIS	*Center for Internet Security*
CISS	*CMS Integrated Security Suite*

CISSP	*Certified Information Systems Security Professional*
CM	*Configuration Management*
CMP	*Configuration Management Plan*
CMS	*Centers for Medicare and & Medicaid Services*
CO	*Central Office*
COB	*Coordination of Benefits*
COMSEC	*Communication Security*
CP	*Contingency Plan (or Planning)*
CPIC	*Certification Package for Internal Controls*
CPU	*Central Processing Unit*
CSAT	*Computer Security Awareness Training*
CSIRC	*Computer Security Incident Response Capability*
CSR	*Core Security Requirement*
CVE	*Common Vulnerability and Exposure*
CWF	*Common Working File*

D

DASD	*Direct Access Storage Devices*
DBA	*Database Administrators*
DBM	*Database Management*
DBMS	*Database Management System*
DC	*Data Center (or District of Columbia)*
DES	*Data Encryption Standard*
DHHS	*Department of Health and Human ServicesSee HHS*
DIR	*Directed (by CMS)*
DISA	*Defense Investigative Security Agency*
DMEMAC	*Durable Medical Equipment Medicare Administrative Contractor*
DNS	*Domain Name System*
DOS	*Denial of Service*
DSL	*Digital Subscriber Line*
DSS	*Digital Signature Standard*

E

EDC	*Enterprise Data Center*
EDI	*Electronic Data Interchange*
EDP	*Electronic Data Processing*
EF	*Exposure Factor*
E-mail	*Electronic Mail*
EO	*Executive Orders*
EVA	*External Vulnerability Assessment*

F

FAR	*Federal Acquisition Regulation*
FE	*FISMA Evaluation*
FFS	*Fee-for-Service*
FIPS	*Federal Information Processing Standards*
FIS	*Federal Information System Controls Audit Manual*
FISCAM	*Federal Information System Controls Audit Manual*
FISMA	*Federal Information Security Management Act of 2002*
FOIA	*Freedom of Information Act*
FMFIA	*Federal Managers' Financial Integrity Act of 1982*
FTI	*Federal Tax Information (or Federal tax return information)*
FY	*Fiscal Year*

H

H	*High*
HHS	*Department of Health and Human Services*
HIPAA	*Health Insurance Portability and Accountability Act*
HISM	*Handbook of Information Security Management*
HITR	*HCFA Information Technology Reference*
HSPD	*Homeland Security Presidential Directive*

I

IA	*Information Assurance (or Identification and Authentication)*
IBM	*International Business Machines (Corp.)*
ID	*Identification (or Identifier)*
IDS	*Intrusion Detection System*
INFOSEC	*Information Systems Security*
IP	*Internet Protocol*
IR	*Incident Response*
IPL	*Initial Program Load*
IRC	*Internal Revenue Code*
IRS	*Internal Revenue Service*
IRSAP	*Internal Revenue Service Acquisition Procedure*
IS	*Information Security*
ISSO	*Information Systems Security Officer*
IT	*Information Technology*
ITL	*Information Technology Laboratory*
ITMRA	*Information Technology Management Reform Act*

L

L	*Low*

M

M	*Moderate*
MA	*Major Application (or Maintenance)*
MAC	*Medicare Administrative Contractor*
MBI	*Minimum Background Investigation*
MBSA	*Microsoft Baseline Security Analyzer*
MCM	*Medicare Carriers Manual*
MCS	*Multiple Console Support*
MDCN	*Medicare Data Communications Network*
MIM	*Medicare Intermediary Manual*
MISPC	*Minimum Interoperability Specification for PKI Components*
MMA	*Medicare Prescription Drug, Improvement, and Modernization Act of 2003*
MP	*Media Protection*
MPS	*Minimum Protection Standard*
MVS	*Multiple Virtual Storage*

N

N/A	*Not Applicable*
NARA	*National Archives and Records Administration*
NC	*Network Computer*
NCSC	*National Computer Security Center*
NIE	*Net Impact Estimate*
NIPC	*National Infrastructure Protection Center*
NIST	*National Institute of Standards and Technology*
NISTIR	*National Institute of Standards and Technology Interagency Report*
NOS	*Network Operating System*
NSA	*National Security Agency*
NSC	*National Security Council*
NSTISSI	*National Security Telecommunications and Information Systems Security Committee*
NVA/ST	*Network Vulnerability Assessment/Security Testing*

O

OIG	*Office of Inspector General*
OIS	*Office of Information Services (CMS)*
OMB	*Office of Management and Budget*
OPM	*Office of Personnel Management*

OS	*Operating System*
OTC	*On-Time-Cost*

P

P.L.	*Public Law*
PartA	*Part A Fiscal Intermediary*
PartB	*Part B Carrier*
PC	*Personal Computer*
PDA	*Personal Digital Assistants*
PDD	*Presidential Decision Directive*
PDS	*Partitioned Data Sets*
PE	*Physical and Environmental Protection*
PII	*Personally Identifiable Information*
PIN	*Personal Identification Number*
PISP	*Policy for the Information Security Program*
PIV	*Personal Identity Verification*
PKI	*Public Key Infrastructure*
PL	*Planning*
PM	*Project (Program) Managers*
PO	*Project Officer*
POA&M	*Plan of Action and Milestones*
POC	*Point-of-Contact*
PSC	*Program Safeguard Contractor*
PSGH	*CMS Policy Standards and Guidelines Handbook*
PS	*Planning*
PSO	*Physical Security Officer*
PUB	*Publication*

Q

QIC	*Quality Integrity Contractor*

R

RA	*Risk Assessment*
RAC	*Recovery Audit Contractor*
RAID	*Redundant Array of Independent Disks*
RAM	*Random Access Memory*
RFP	*Requests for Proposals*
RO	*Regional Office*
ROM	*Read Only Memory*

S

SA	*Security Administrator (or System and Services Acquisition)*
SAR	*Safeguard Activity Report*
SAS	*Statement on Auditing Standard*
SBI	*Single Scope Background Investigation (SBI)*
SBU	*Sensitive but unclassified*
SC	*Security Category (or System and Communications Protection)*
SCHIP	*State Children's Health Insurance Program*
SDLC	*System Development Life Cycle*
SER	*Scientific, Engineering, and Research*
SHS	*Secure Hash Standard*
SI	*System and Information Integrity*
SII	*Security/Suitability Investigation Index*
SIRT	*Security Incident Response Team*
SLE	*Single Loss Expectancy*
SM	*System Manager*
SMF	*System Management Facility*
S-MIME	*Secure Multi-purpose Internet Mail Extensions*
SOW	*Statement of Work*
SP	*Special Publication*
SPR	*Safeguard Procedures Report*
SS	*Standard System [Maintainer]*
SSA	*Social Security Administration*
SSC	*Systems Security Coordinator*
SSL	*Secure Socket Layer*
SSM	*Shared System Maintainers*
SSO	*Systems Security Officer*
SSP	*System Security Plan*
SSPM	*System Security Plans Methodology*
SSSA	*Senior Systems Security Advisor*
ST&E	*Security Test and Evaluation*
STIG	*Security Technical Implementation Guide*

T

TCP	*Transmission Control Protocol*
TDES	*Triple Data Encryption Algorithm*
TLS	*Transport Layer Security*
TO	*Training Office*

U

U.S.C.	*United States Code*
UID	*User Identification*
UL	*Underwriter's Laboratory*

V

VPN	*Virtual Private Network*

Z

ZPIC	*Zone Program Integrity Contractor*

Appendix H:
Glossary

(Rev. 9, 06-20-08)

Term	Definition
Access	*Ability to make use of any information system (IS) resource. (NIST SP 800-32)*
Access Control	*The process of granting or denying specific requests:* *(i) obtain and use information and related information processing services; and* *(ii) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances). (FIPS 201)*
Access Control List (ACL)	*A list of entities that are authorized to have access to a resource, together with their access methods.*
Access Control Software	*S*oftware (CA-ACF2, RACF, CA-TOP SECRET), which is external to the operating system, provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection such as denying access for which the user is not expressly authorized, allowing access which is not expressly authorized but providing a wanting, or allowing access to all resources without warning regardless of authority. (FISCAM)
Account Management	*Involves:* *(i) the process of requesting, establishing, issuing, and closing user accounts;* *(ii) tracking users and their respective access authorizations; and* *(iii) managing these functions. (NIST SP 800-12)*
Accountability	*The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (NIST SP 800-27A)*

Accreditation	(1) *The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (FIPS 200)* (2) *The formal declaration by the DAA that a major application or general support system is granted approval to process using a prescribed set of safeguards in a specific operational environment. The accreditation decision is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate security after the implementation of an agreed upon set of security controls. (NIST SP 800-18)*
Adequate Security	*Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. (FIPS 200; OMB Circular A-130, App. III)*
Adequately Met	*Includes:* *(i) functionality that performs correctly,* *(ii) sufficient protection against unintentional errors (by users or software), and* *(iii) sufficient resistance to intentional penetration or by-pass. (NIST SP 800-27A)*
Administrative Access	*An advanced level of access to a computer or application that includes the ability to perform significant configuration changes to the computer's operating system. Also referred to as "privileged access" or "root access." (NIST SP 800-40)*
Administrative Safeguards	*Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. (NIST SP 800-66)*
Advanced Encryption Standard (AES)	*Specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. (NIST SP 800-46)* *Note: Through 2030, TDEA and AES will coexist as FIPS-approved algorithms, allowing for a gradual transition to AES.*
AES	*See Advanced Encryption Standard.*
Alternate Site	*An operating location other than the one at which an activity is usually performed for use by business functions when the primary facilities are unavailable.*

Application	*(1) The use of information resources (information and information technology) to satisfy a specific set of user requirements. (NIST SP 800-37)* *(2) Any data entry, update, query, or report program that processes data for the user. (NIST SP 800-40)*
Approved (Algorithm or Cryptography)	*FIPS approved or NIST recommended. An algorithm or technique that is either:* *(i) specified in a FIPS or a NIST recommendation or* *(ii) adopted in a FIPS or NIST recommendation. (FIPS 201)* *There are only two (2) Approved encryption algorithms allowed within CMS system environments: AES and Triple DES.*
Architecture	*A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability). (FIPS 201)*
Assessment Findings	*Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition. (NIST SP 800-53A)*
Assessment Method	*A focused activity or action employed by an assessor for evaluating a particular attribute of a security control. (NIST SP 800-37; NIST SP 800-53R1)*
Assessment Procedure	*A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (NIST SP 800-37; NIST SP 800-53R1)*
Asset	*(1) A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems. (NIST SP 800-26)* *(2)* Any software, data, hardware, administrative, physical communications, or personnel resource within an ADP system of activity.

Assurance	*One of the five (5) "Security Goals." It involves support for our confidence that the other four (4) security goals (integrity, availability, confidentiality, and accountability) have been "adequately met" by a specific implementation. (NIST SP 800-27A)* *Also see Adequately Met.*
Attack	*Attempt to gain unauthorized access to an IS's services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality. (CNSSI 4009)*
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (*NIST SP 800-32;* CNSS*I 4009*)
Audit Data	*Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. (NIST SP 800-32)*
Audit Reduction Tools	*Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. (NIST SP 800-12)*
Audit Trail	*(1) A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period. (NIST SP 800-47)* *(2) Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. (CNSSI 4009)*
Authenticate	*To confirm the identity of an entity when that identity is presented. (NIST SP 800-32)*
Authentication	*(1) Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (FIPS 200)* *(2) Encompasses identity verification, message origin authentication, and message content authentication. (FIPS 190)*
Authentication Mechanism	*Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device. (NIST SP 800-72)*

Authorization	*The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)*
Authorizing Official	*Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority. (FIPS 200)*
Automated Labeling	*Refers to labels employed on internal data structures (e.g., records, files) within the information system. (NIST SP 800-53R1)*
Automated Marking	*Refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in automated labeling. (NIST SP 800-53R1)*
Availability	*Ensuring timely and reliable access to and use of information. (44 U.S.C., Sec. 3542)*
Awareness	*Activities which seek to focus an individual's attention on an (information security) issue or set of issues. (NIST SP 800-50)*
Background Investigation (BI)	*This is a more in-depth version of the LBI since the personal investigation coverage is the most recent five (5) to seven (7) years. This investigation is required of those going into "high risk" public trust positions. (OPM)*
Backup	*A copy of files and programs made to facilitate recovery if necessary. (CNSSI 4009)*
Baseline Configuration	*Includes information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. Also includes a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs / objectives. (NIST SP 800-53R1)*
Basic Input/Output System (BIOS)	*The program that starts up your computer and communicates between the devices in your computer (such as your hard drive and graphics card) and the system.*

Best Practices	*The processes, practices, or systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency. (GAO Assessing Risks and Returns: A Guide for Evaluation Agencies' IT Investment Decision-making)*
Biometric	*A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics. (FIPS 201)*
Boundary Protection	*Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization and information systems not completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). (NIST SP 800-53R1)*
Browsing	(1) The act of electronically perusing files and records without authorization. (FISCAM) (2) The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (*CNSSI 4009*)
Business Continuity Plan (BCP)	*The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. (NIST SP 800-34)*
Business Impact Analysis (BIA)	*An analysis of an IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (NIST SP 800-34)*

Business Owner	*(1) Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST SP 800-53A)* *(2) Component or individual who have primary ownership of a major CMS business function or process. Examples are Medicare contractors, Program Safeguard Contractors, Shared Systems, Quality Improvement Organizations, Survey & Certification, Medicare Advantage Contractors, Medicare Call Centers, Enterprise Data Centers, and organizations conducting CMS sponsored research.*
Business Recovery /Resumption Plan (BRP)	*The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred. (NIST SP 800-34)*
Certificate Policy	*A specialized form of administrative policy tuned to electronic transactions performed during certificate management. It addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. (NIST SP 800-32)*
Certification (Recertification)	*A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (FIPS 200)*
Certification Agent	*The individual, group, or organization responsible for conducting a security certification. (NIST SP 800-53R1)*
Certification and Accreditation (C&A)	*A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)*

Certification Authority (CA)	*A trusted entity that issues and revokes public key certificates. (FIPS 201)*
Certification Practice Statement (CPS)	*A statement of the practices that a Certification Authority employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services). (NIST SP 800-32)*
Chain of Custody	*A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. (NIST SP 800-72)*
Change Request	*A request to modify any aspect of a system or environment including baseline requirements, hardware, or software.*
Chief Information Officer (CIO)	*Agency official responsible for:* *(i) Providing advice and other assistance to the head of the executive agency [or organization] and other senior management personnel of the agency [or organization] to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency [or organization];* *(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency [or organization]; and* *(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency [or organization], including improvements to work processes of the agency [or organization]. (FIPS 200; P.L. 104-106, Sec. 5125(b))*
Clear	*To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. (NIST SP 800-88)*
Client (Application)	*A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server. (NIST SP 800-32)*
Code	Instructions written in a computer programming language. (FISCAM) *Also see Object Code and Source Code.*

Cold Site	*A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site. (NIST SP 800-34)*
Collaborative Computing	*Applications and technology (e.g. , whiteboarding, group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment. (CNSSI 4009)*
Common Vulnerabilities and Exposures (CVE)	*A dictionary of common names for publicly known IT system vulnerabilities. (NIST SP 800-51)*
Compensating *Security* Control*(s)*	*The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53R1 (i.e., CSRs, ARS), that provide equivalent or comparable protection for an information system. (NIST SP 800-53R1)*
Compromise	*Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (NIST SP 800-32)*
Computer Forensics	*The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (NIST SP 800-61)*
Computer Security Incident	*A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. (NIST SP 800-61)*
Computer Security Incident Response *Team* (*CSIRT*)	*A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).* (NIST SP 800-*61*)
Confidentiality	*Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (44 U.S.C., Sec. 3542)*
Configuration Control	*Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation. (CNSSI 4009)*
Console	Traditionally, a control unit such as a terminal through which a user *communicates* with a computer. In the mainframe environment, a *console* is the operator's station. (FISCAM)

Consortium	Currently consists of four *(4)* CMS offices (Northeastern, Southern, Midwestern, and Western) that oversee the operations at the Regional Offices.
Contingency Plan ***(CP)***	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure*s*, or disaster. *(NIST SP 800-34)*
Contingency Planning	See *C*ontingency *P*lan.
Continuity of Operations Plan (COOP)	*A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to thirty (30) days as a result of a disaster event before returning to normal operations. (NIST SP 800-34)*
Control Technique*s*	Statements that provide a description of what physical, software, procedural or people related condition *shall* be met or in existence in order to satisfy a core requirement.
Controlled Area	*Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. (NIST SP 800-53A)*
Cookie	*A piece of information supplied by a Web server to a browser, along with requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. (NIST SP 800-46)*
Countermeasures	*Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. (FIPS 200; CNSSI 4009)*
Coverage	*An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). (NIST SP 800-53A)*
Credential	*An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. (NIST SP 800-63)*
Credit Check	*This is an automated credit record search conducted through various major credit bureaus. It is included in most background investigations except the basic NACI investigation required of employees entering Non-Sensitive (Level 1) positions. (HHS Personnel Security/Suitability Handbook)*
Critical Assets	*Those physical and information assets required for the performance of the site mission. (HHS IRM Policy)*
Critical Infrastructure	*Physical and cyber-based systems essential to the minimum operations of the economy and government. (PDD-63)*

Criticality Level	*Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level. (NIST SP 800-60)*
Cryptographic Algorithm	*A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. (FIPS 140-2)*
Cryptographic Key (Key)	*A parameter used in conjunction with a cryptographic algorithm that determines:* • *The transformation of plaintext data into ciphertext data,* • *The transformation of ciphertext data into plaintext data,* • *A digital signature computed from data,* • *The verification of a digital signature computed from data,* • *An authentication code computed from data, or* • *An exchange agreement of a shared secret. (FIPS 140-3)*
Cryptographic Module	*The set of hardware and/or software that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. (NIST SP 800-32; FIPS 140-3)*
Cryptography	*The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. (NIST SP 800-21)*
Data	*Programs, files or other information stored in, or processed by, a computer system. (FIPS 112)*
Data Element	*A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. (NIST SP 800-47)*
Data Encryption Algorithm (DEA)	*The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)*
Data Encryption Standard (DES)	*The symmetric encryption algorithm that serves as the cryptographic engine for the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)* *Note: The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP 800-46)*
Data Integrity	*The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (NIST SP 800-27A)*
Data Owner	See *Information* Owner.

Data Security	The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (FIPS 39) *Also s*ee Security Management Function.
Degauss	*To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors. (NIST SP 800-88)*
Demilitarized Zone (DMZ)	*A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks. (NIST SP 800-41)*
Denial of Service (DOS)	*The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) (NIST SP 800-27A)*
Depth	*An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. (NIST SP 800-53A)*
Destruction	*The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive. (NIST SP 800-88)*
Digital Signature	*The result of a cryptographic transformation of data which, when properly implemented, provides the services of:* • *Origin authentication,* • *Data integrity, and* • *Signer non-repudiation (FIPS 140-3)*
Disaster Recovery Plan *(DRP)*	*A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. (NIST SP 800-34)*
Discretionary Access Control	*The basis of this kind of security is that an individual user, or program operating on the user's behalf is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. (FIPS 191)*
Disposal	*Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media. (NIST SP 800-88)*

Disruption	*An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (NIST SP 800-34)*
Distributed Denial of Service (DDoS)	*A Denial of Service technique that uses numerous hosts to perform the attack. (NIST SP 800-61)*
Domain	*A set of subjects, their information objects, and a common security policy. (NIST SP 800-27A)*
Electronic Authentication (E-authentication)	*The process of establishing confidence in user identities electronically presented to an information system. (NIST SP 800-63)*
Electronic Mail (email)	*A store and forward method of composing, sending, storing, and receiving messages over electronic communication systems. The term "email" (as a noun or verb) applies both to the Internet email system based on the Simple Mail Transfer Protocol (SMTP) and to X.400 systems, and to intranet systems allowing users within one organization to email each other. Often these workgroup collaboration organizations may use the Internet protocols or X.400 protocols for internal email service. Email is often used to deliver bulk unsolicited messages, or "spam", but filter programs exist which can automatically delete some or most of these, depending on the situation. (Wikipedia)*
Electronic Media	*(1) General term that refers to media on which data are recorded via an electrically based process. (NIST SP 800-88)* *(2) Electronic storage media including memory devices in computers (hard drives) and any removable /transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or* *Transmission media used to exchange information already in electronic storage media (e.g., Internet, extranet, leased lines, dial-up lines, private networks, and the physical movement of removable /transportable electronic storage media. (HIPAA)*
Electronic Protected Health Information (EPHI)	*Individually identifiable health information that is:* *(i) transmitted by electronic media, or* *(ii) maintained in electronic media. (HIPAA)*

Electronic Signature	A symbol, generated through electronic means, that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria. (FISCAM)
Encryption	*Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. (FIPS 185)*
Entity	*(1) Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). (NIST SP 800-27A)* *(2) An individual (person), organization, device or process. (NIST SP 800-57, Part 1)*
Environment	*Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. (FIPS 200; CNSSI 4009)*
Event	*Any observable occurrence in a network or system. (NIST SP 800-61)*
Examine	*A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time. (NIST SP 800-53A)*
External Information System (or Component)	*An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (NIST SP 800-53A)*
External Information System Service	*An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). (NIST SP 800-53A)*
External Information System Service Provider	*A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (NIST SP 800-53A)*

Extranet	*A virtual network created by connecting two intranets. An organization that connects remote locations with a VPN creates an extranet by linking its intranets together to form one virtual network. (NIST SP 800-41)*
Federal Information System	*An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (40 U.S.C., Sec. 11331)*
File	*A collection of information logically grouped into a single entity and referenced by a unique name, such as a filename. (NIST SP 800-111)*
General Support System(s) (GSS)	An interconnected set of information resources under the same direct management control which shares common functionality. *It* normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network. A departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. (*NIST SP 800-53R1;* OMB Circular A-130*, App. III*)
Guided Media	*Medium* in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable*, optical fiber*) *providing a closed path between sender and receiver.* (Computer Assisted Technology Transfer Laboratory, Oklahoma State University)
Handled	(As in *"*Data handled.*"*) Stored, processed or used in an ADP system or communicated, displayed, produced, or disseminated by an ADP system.
High-Impact System	*An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. (FIPS 200)*
Hot Site	A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster. (*NIST SP 800-34*)
Hotfix	*Microsoft's term for a security patch. (NIST SP 800-40)* *Also see Patch.*
Identification	*(1) The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. (NIST SP 800-47)* *(2) The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. (FIPS 201)*

Identifier	*A unique data string used as a key in the biometric system to name a person's identity and its associated attributes. (FIPS 201)*
Identity	*(1) A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person shall include sufficient additional information to make the complete name unique. (NIST SP 800-63)* *(2) The set of physical and behavioral characteristics by which an individual is uniquely recognizable. (FIPS 201)*
Image	*An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered. (NIST SP 800-72)*
Impact	*The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (NIST SP 800-60, Vol. 2)*
Inappropriate Usage	*A person who violates acceptable computing use policies. (NIST SP 800-61)*
Incident	*(1) The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction.* *(2) An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (FIPS 200)*
Incident Handling	*The mitigation of violations of security policies and recommended practices. (NIST SP 800-61)*
Incident Response Plan	*The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT system(s). (NIST SP 800-34)*
Incineration	*A physically destructive method of sanitizing media; the act of burning completely to ashes. (NIST SP 800-88)*
Incremental Backup	*The process of making a copy of only the files that have changed since the last backup instead of backing up every file.*

Independent Certification Agent or Team	*Any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. (NIST SP 800-53A)*
Individual	*(1) An assessment object that includes people applying specifications, mechanisms, or activities. (NIST SP 800-53A)* *(2) Person who is the subject of protected health information (PHI). (HIPAA)*
Information	(1) *An instance of an information type. (FIPS 200)* (2) Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (OMB Circular A-130)
Information Assurance	*Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (CNSSI-4009)*
Information Owner	*Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. (NIST SP 800-53R1; CNSSI 4009)*

Information Remnance	*Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user / role (or the actions of a process acting on behalf of a prior user / role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. (NIST SP 800-53R1)*
Information Resource Owner	See *Business* Owner.
Information Resource*s*	*Information and related resources, such as personnel, equipment, funds, and information technology. (44 U.S.C., Sec. 3502)*
Information Security	*The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (44 U.S.C., Sec. 3542)*
Information Security Agreement (ISA)	*An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a memorandum of understanding or agreement (MOU/A) between the organizations. (NIST SP 800-26)*
Information Security Policy	*Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. (CNSSI 4009)*
Information Sharing	*A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C., Sec. 3502; OMB Circular A-130, App. III)*
Information System	*(1) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C., Sec. 3502* *(2) An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. (HIPAA)*
Information System Owner (or Program Manager)	*See Business Owner.*

Information System Security Officer (ISSO)	(1) Individual responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with *System Security Officer (SSO)*. *(2) Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (NIST SP 800-53R1)*
Information Technology (IT)	*Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:* *(i) requires the use of such equipment; or* *(ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.* *The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. (40 U.S.C., Sec. 1401)*
Information Type	*A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. (FIPS 199)*
Inside Threat	*An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. (NIST SP 800-32)*
Integrity	*(1) Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (44 U.S.C., Sec. 3542)* *(2) The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. (FIPS 140-2)*

Interconnection Security Agreement (ISA)	*An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. (NIST SP 800-47)*
Internet	When capitalized, the term "Internet" refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. (FISCAM)
Interview	*A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time. (NIST SP 800-53A)*
Intranet	*A network internal to an organization but that runs the same protocols as the network external to the organization. Every organizational network that runs the TCP/IP protocol suite is an intranet. (NIST SP 800-41)*
Intrusion Detection System (IDS)	*Software that looks for suspicious activity and alerts administrators. (NIST SP 800-61)*
Intrusion Prevention System	*System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. (NIST SP 800-36)*
IP Security (IPsec)	*Request For Comments (RFC) 2411, protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol is used to negotiate the secret keys that protect Virtual Private Network (VPN) communications, and the level and type of security protections that will characterize the VPN. The most widely used key management protocol is the Internet Key Exchange (IKE) protocol. (NIST SP 800-46)*
Key	*See Cryptographic Key.*
Key Management	*The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. (FIPS 140-2)*
Keystroke Monitoring	*The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. (NIST SP 800-26)*
Label	*Information associated with a key that identifies the key's parameters attributes or intended use. (NIST SP 800-57, Part 1)* *Also see Security Label.*

Least Privilege	*The security objective of granting users only those accesses they need to perform their official duties. (NIST SP 800-12; NIST SP 800-26)*
Limited Background Investigation (LBI)	This investigation consists of a NACI*C*, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three *(3)* years. (*OPM*)
Link Encryption	*Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing. (NIST SP 800-12)*
Local Access	*Access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. (NIST SP 800-53A)*
Log(s)	With respect to computer systems, to record an event or transaction. (FISCAM) *Also see Record(s).*
Low-Impact System	*An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. (FIPS 200)*
Major Application (MA)	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (OMB Circular A-130*, App. III*) All "Major Applications" require "special management attention." The System Security Plan for a Major Application may be defined broadly enough to include hardware, software, networks, and even facilities where it is reasonable. This permits the systems to be bounded in reasonable ways for the purposes of security planning.
Malicious Code	*Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of*

	malicious code. (NIST SP 800-61; CNSSI 4009)
Malware	*A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (NIST SP 800-83)*
Management Controls	*The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. (FIPS 200)*
Mandatory Access Control	*(1) A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. (NIST SP 800-44)* *(2) Access controls (which) are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information. (FIPS 191)*
Mechanisms	*An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system. (NIST SP 800-53A)*
Media	*(1) Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (FIPS 200)* *(2) Includes both digital media (e.g., diskettes, magnetic tapes, external / removable hard drives, flash / thumb drives, compact disks [CD], digital video disks [DVD]) and non-digital media (e.g., paper, microfilm). (NIST SP 800-53R1)*
Media Sanitization	*A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (NIST SP 800-88)*
Medium	*Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. (NIST SP 800-88)*
Memorandum of Understanding /Agreement (MOU/A)	*A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (NIST SP 800-47)*

Metrics	*Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. (NIST SP 800-55)*
Minimum Background Investigation (MBI)	This investigation includes a *NACIC*, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. *(OPM)*
Mission Critical	*Any telecommunications or information system that is defined as a national security system (i.e., FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency. (NIST SP 800-60, Vol. 2)*
Mobile Code	*Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. (NIST SP 800-53A)*
Mobile Code Technologies	*Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript, PDF, Shockwave movies, Flash animations). (NIST SP 800-53A)*
Moderate-Impact System	*An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. (FIPS 200)*
National Agency Check (NAC)	*An integral part of all background investigations, consisting of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. (OPM)*
National Agency Check and Inquiries (NACI)	*The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five (5) years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). (OPM)*
National Agency Check and Inquiries and Credit (NACIC)	*Includes the NACI with the addition of a credit record search. (OPM)*
Need-To-Know	The necessity for access to, or knowledge or possession of, specific information required to carry out official duties. (CNSS*I 4009*)

Non-repudiation	*Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (NIST SP 800-39)*
Object	*A passive entity that contains or receives information. (NIST SP 800-27A)*
Office of Information Systems (OIS)	*CMS office that ensures the effective management of CMS's information systems and resources. The office also develops and maintains central databases and statistical files, and directs Medicare claims payment systems.*
Off-site Storage Facility	*A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored for backup or other purposes.*
Operating System (OS)	*The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its principal component, the kernel, resides in memory at all times. The OS sets the standards for all application programs (such as the mail server) that run in the computer. The applications communicate with the OS for most user interface and file management operations. (NIST SP 800-45)*
Operational Controls	*The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). (FIPS 200)*
Organization	*A federal agency or, as appropriate, any of its operational elements. (FIPS 200)*
Outside Threat	*An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. (NIST SP 800-32)*
Overwrite	*Writing patterns of data on top of the data stored on a magnetic medium. NSA has researched that one overwrite is good enough to sanitize most drives. (NIST SP 800-88)*
Password	(1) *A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. (NIST SP 800-63)* *(2) A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. (FIPS 181)* (*3*) *A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. (FIPS 140-3)*
Patch	*An additional piece of code developed to address a problem in an existing piece of software. (NIST SP 800-40)*

Penetration	Unauthorized act of bypassing the security mechanisms of a system. (CNSS*I 4009*)
Penetration Test	*A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. (NIST SP 800-53A)*
Personal Identification Number (PIN)	*A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits. (FIPS 201)*
Personal Identity Verification Card (PIV Card)	*Physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). (FIPS 201)*
Personally Identifiable Information (PII)	*Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual.*
Phishing	*Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. (NIST SP 800-83)*
Physical Destruction	*A sanitization method for optical media, such as CDs. (NIST SP 800-88)*
Plaintext	*Intelligible data that has meaning and can be understood without the application of decryption. (NIST SP 800-21)*
Plan of Action and Milestones	*A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (OMB M-02-01)*
Policy	*An official statement of a position, plan or course of action established by an identified sponsoring authority, which is designed to influence, to provide direction and to determine decisions and actions with regard to a specific topic. Policies provide broad direction or goals. Standards, procedures and guidelines flow from policies.* *Also see Security Policy.*

Portable and Mobile Devices	*Includes notebook computers, personal digital assistants, cellular telephones; and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations. (NIST SP 800-53R1)*
Position Sensitivity	*The degree of risk and level of relative importance assigned to a specific position. (HHS Personnel Security/Suitability Handbook)*
Potential Impact	*The loss of confidentiality, integrity, or availability could be expected to have:* *(i) a limited adverse effect (FIPS 199 low);* *(ii) a serious adverse effect (FIPS 199 moderate); or* *(iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. (NIST SP 800-39, FIPS 199 Adapted)*
Privacy Impact Assessment (PIA)	*An analysis of how information is handled:* *(i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,* *(ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and* *(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. (NIST SP 800-60, OMB M-03-22)*
Privacy Information	The individual's right to privacy must be protected in Federal Government information activities involving personal information. Such information is to be collected, maintained, and protected so as to preclude intrusion into the privacy of individuals and the unwarranted disclosure of personal information. (OMB Circular A-130)
Privileged Accounts	*Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts. (NIST SP 800-12)*
Privileged Function	*A function executed on an information system involving the control, monitoring, or administration of the system. (NIST SP 800-53A)*
Privileged User	*Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, information system security officer, maintainer, system programmer). (CNSSI 4009)*
Procedures	*(1) A course of action to be taken to perform a given task.* *(2) A particular method or guidance for implementing a policy or performing a task or operation which has to be executed in the same manner in order to always obtain the same result in the same circumstance (e.g., emergency procedure). (Internet)*

Production Programs	Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from "test" programs that are being developed or modified, but have not yet been authorized for use by management. (FISCAM)
Profile	A set of rules that describes the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks. *(FISCAM)* *Also s*ee Standard Profile and User Profile.
Protected Health Information (PHI)	*Individually identifiable health information that is:* *(i) transmitted by electronic media,* *(ii) maintained in electronic media, or* *(iii) transmitted or maintained in any other form or medium. (HIPAA)* *NOTE: PHI excludes individually identifiable health information in employment records held by a covered HIPAA entity in its role as employer.*
Proxy	*A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, an Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and an Simple Mail Transfer Protocol (SMTP) proxy used for e-mail. (NIST SP 800-44)*
Public Information	*Any information, regardless of form or format that an agency discloses, disseminates, or makes available to the public. (NIST SP 800-60, Vol. 2)*
Public Key Certificate	*(1) A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. (NIST SP 800-63)* *(2) A set of data that contains a unique identifier associated with an entity, contains the public key associated withy the identifier, and is digitally signed by a trusted party, thereby binding the public key to the identifier. (FIPS 140-3)*

Public Key Infrastructure (PKI)	*An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys. (FIPS 196)*
Pulverization	*A physically destructive method of sanitizing media; the act of grinding to a powder or dust. (NIST SP 800-88)*
Purge	*Rendering sanitized data unrecoverable by laboratory attack methods. (NIST SP 800-88)*
Quality Assurance	The function that reviews software project activities and tests software products throughout the software life-cycle to determine if*:* (*i*) the software project is adhering to its established plans, standards, and procedures, and (*ii*) the software meets the functional specifications defined by the user. (FISCAM)
Record*(s)*	*(1) The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). (FIPS 200)* *(2)* A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item. (FISCAM)
Recovery Procedures	Actions necessary to restore data files of an information system and computational capability after a system failure. (CNSS*I 4009*)
Remanence	*Residual information remaining on storage media after clearing. (NIST SP 800-88)*
Remediation	*The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application. (NIST SP 800-40)*
Remote Access	*Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. (NIST SP 800-53R1)*
Remote Maintenance	*Maintenance and diagnostic activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). (NIST SP 800-53A)*

Remote Session	*A session initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). (NIST SP 800-53R1)*
Residual Risk	*The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat. (NIST SP 800-33)*
Residue	*Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place. (NIST SP 800-88)*
Resource	*See Information Resource.*
Resource Owner	See *Business* Owner.
Risk	*The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (FIPS 200 Adapted)*
Risk Analysis	(1) The identification and study of the vulnerability of a system and the possible threats to its security. (FIPS 11-3) (2) *The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. (NIST SP 800-27A)*
Risk Assessment	*The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in-place security controls. (NIST SP 800-30 Adapted)*
Risk Management	(1) A management approach designed to reduce risks inherent to system development and operations. (FISCAM) (2) *The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:* *(i) the conduct of a risk assessment;* *(ii) the implementation of a risk mitigation strategy; and* *(iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (FIPS 200 Adapted)*

Risk Mitigation	*Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. (NIST SP 800-30)*
Risk Tolerance	*The level of risk an entity is willing to assume in order to achieve a potential desired result. (NIST SP 800-32)*
Safeguard*s*	*Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. (FIPS 200)*
Sanitize (or Sanitization)	*Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. (NIST SP 800-88)*
Scenario	*A functional exercise staff member who simulates or represents non-participating individuals or organizations whose input or participation is necessary to the flow of the exercise. (NIST SP 800-84)*
Secure Name / Address Resolution Service (Authoritative Source)	*Enables remote clients to obtain origin authentication and integrity verification assurances for the name / address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name / address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure DNS deployment. (NIST SP 800-53R1)*
Secure Name / Address Resolution Service (Recursive or Caching Resolver)	*An information system that provides name / address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST SP 800-81 provides guidance on secure domain name system deployment. (NIST SP 800-53R1]*
Secure Sockets Layer (SSL)	*Protocol based on public key cryptography. Used to generate a cryptographic session that is private to a Web server and a client browser. (NIST SP 800-41)*
Security Accreditation	*The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)*

Security Assessment	*The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (NIST SP 800-53A)*
Security Attribute	*A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes. (FIPS 188)*
Security Category	*The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. (FIPS 199; FIPS 200)*
Security Certification	A formal testing of the security safeguards implemented in the computer system to determine whether they meet applicable requirements and specifications. To provide more reliable technical information, certification is often performed by an independent reviewer, rather than by the people who designed the system. (NIST *SP* 800-12)
Security Communications Protocol	*A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection. (NIST SP 800-57)*
Security Control Baseline	*The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. (FIPS 200)*
Security Control Enhancements	*Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. (NIST SP 800-53A)*
Security Controls	*The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (FIPS 199; FIPS 200)*
Security Domain	*(1) A set of subjects, their information objects, and a common security policy. (NIST SP 800-27A)* *(2) A collection of entities to which applies a single security policy executed by a single authority. (FIPS 188)*
Security Functions	*The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based. (NIST SP 800-53A)*

Security Impact Analysis	*The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system. (NIST SP 800-37)*
Security Incident	*A security incident is a violation, or an imminent threat of a violation, of an explicit or implied security policy, acceptable use policies, or standard security practices.* *Also see Incident.*
Security Label	*Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein. (NIST SP 800-53A)*
Security Level	*A hierarchical indicator of the degree of sensitivity to a certain threat. It implies, according to the security policy being enforced, a specific level of protection. (FIPS 188)*
Security Objective	*Confidentiality, integrity, or availability. (FIPS 199; FIPS 200)*
Security Plan	*See System Security Plan (SSP).*
Security Policy	*(1) A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance. (Federal IT Security Assessment Framework)* *(2) A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. (FIPS 188)*
Security Requirements	*Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. (FIPS 200)*
Security Requirements Baseline	Description of the minimum requirements necessary for an information system to maintain an acceptable level of security. (CNSS*I 4009*)
Security Service	*(1) A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication. (NIST SP 800-27A)* *(2) Mechanism used to provide confidentiality, data integrity, authentication or non-repudiation of information. (NIST SP 800-57, Part 1)*

Security Test and Evaluation (ST&E)	*An examination and analysis of the security safeguards of a system as they have been applied in an operational environment in order to determine the security posture of the system.*
Security Testing	*A process that is used to determine that the security features of a system are implemented and functioning as designed. This process includes hands on functional testing, penetration testing and verification.*
Sensitive Information	(1) Any information whose loss, misuse, unauthorized access, unauthorized disclosure, or improper modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. (FISCAM) (2) *Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act. (NIST SP 800-26)* (3) CMS Sensitive Information corresponds to *a* "High*" system security level as* described in section 4.*0* of this document.
Sensitivity Levels	*A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted. (FIPS 201)*
Separation of Duties / Segregation of Duties	*To ensure that no single person has control of a transaction from beginning to end and that two or more people are responsible for its execution. This is intended to prevent one person from manipulating transactions for personal gain.*
Service *C*ontinuity *C*ontrols	This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. (FISCAM)
Session	*A session is an encounter between an end-user interface device (e.g., computer, terminal, process) and an application, including a network logon. One user session is the time between starting the application and quitting. (Multiple sources)*
Session Control	*The application of security mechanisms to network connections which are intended to prevent unauthorized persons from capturing or modifying network connection data, or taking control of pre-established network connections.*

Shred	*A method of sanitizing media; the act of cutting or tearing into small particles. (NIST SP 800-88)*
Signature	*A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system. (NIST SP 800-61)*
Signed Data	*Data on which a digital signature is generated. (FIPS 196)*
Significant Change	A physical, administrative, or technical modification that alters the degree of protection required. *Examples include, but are not limited to, changes in operating systems, computer hardware, firmware, operational environment, or system boundaries; new services or applications; or other conditions that potentially impact the system's security posture or accreditation status. (NIST SP 800-53R1)*
Smart Card	*A credit card with a built-in microprocessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times. (NIST SP 800-48)*
Sniffer	*Software that observes and records network traffic. (NIST SP 800-61) Synonymous with packet sniffer.*
Social Engineering	*An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. (NIST SP 800-61)*
Special Management Attention	Some systems require "special management attention" to security due to the risk and magnitude of the harm that would result from the loss, misuse, unauthorized access to, or modification of the information in the system. (OMB Circular A-130)
Specification	*An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system. (NIST SP 800-53A)*
Spyware	*Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. (NIST SP 800-53A)*
Standard	*A published statement on a topic specifying characteristics, usually measurable, that shall be satisfied or achieved in order to comply with the standard. (FIPS 201)*
Storage	*Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered, and from which data may be retrieved. (NIST SP 800-88)*

Subsystem	*A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions. (NIST SP 800-18)*
Suitability	*Refers to identifiable character traits and conduct sufficient to decide whether an individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate integrity, efficiency, and effectiveness. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, and skills. (OPM)*
System	(*1*) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. (OMB Circular A-130) (*2*) *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (NIST SP 800-53R1)* A system normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people. A system's hardware may include mainframe systems, desktop systems (e.g., PC's, Macintoshes, laptops, handheld devices), workstations and servers (e.g., Unix, NT, NC), local area networks (LAN), and any other platform regardless of the operating system. *Also see Information System.*
System Administrator	*A person who manages the technical aspects of a system. (NIST SP 800v2)*
System Development Life Cycle (SDLC)	*The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (NIST SP 800-34)*
System Integrity	*The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. (NIST SP 800-27A)*
System Interconnection	*The direct connection of two or more IT systems for the purpose of sharing data and other information resources. (NIST SP 800-26)*

System Interconnection	*The direct connection of two or more IT systems for the purpose of sharing data and other information resources. (NIST SP 800-47)*
System Maintainer	*The individual or group of individuals who have the responsibilities of continued maintenance (e.g. bug fixing, minor modifications /enhancements, performance tuning, and/or customer service) of an implemented system. A system maintainer may or may not also serve as the system developer for a given project.*
System Media	*Includes both digital media (e.g., diskettes, magnetic tapes, external / removable hard drives, flash / thumb drives, compact disks [CD], digital video disks [DVD]) and non-digital media (e.g., paper, microfilm). (NIST SP 800-53R1)*
System Security Plan (SSP)	*Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (NIST SP 800-18; FIPS 200)*
System Software	*The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data. (FIPS 140-2)*
System Test	*A test performed on a complete system to evaluate its compliance with specified requirements. (NIST SP 800-84)*
Tabletop Exercise	*A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. (NIST SP 800-84)*
Tailoring	*The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on:* *(i) the application of scoping guidance;* *(ii) the specification of compensating security controls, if needed; and* *(iii) the specification of organization-defined parameters in the security controls, where allowed. (NIST SP 800-53A)*
Technical Controls	*The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. (FIPS 200)*

Telecommunications	*The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received. (NIST SP 800-60, Vol. 2)*
Test	*A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time. (NIST SP 800-53A)*
Test Bed	*Test environment containing the software, data, and simulations necessary for testing systems.*
Test Plan	*A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step. (NIST SP 800-84)*
Threat	*Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (FIPS 200)*
Threat Analysis	*The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment. (NIST SP 800-27A)*
Threat Assessment	*Formal description and evaluation of threat to an information system. (CNSSI 4009)*
Threat Source	*The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent. (FIPS 200)*
Token	*Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity. (NIST SP 800-63)*

Transport Layer Security (TLS)	*A protocol created to provide authentication, confidentiality and data integrity between two communicating applications over the Internet. Although based on the precursor protocol SSL 3.0, TLS is considered an improvement to SSL 3.0. (Adapted from NIST SP 800-52)* *Note: While SSL 3.0 is the most secure of the SSL protocol versions, it is not approved for use in the protection of Federal information because it relies in part on the use of cryptographic algorithms that are not FIPS-approved. TLS, when properly configured, is approved for the protection of Federal information. (NIST SP 800-52)*
Triple Data Encryption Algorithm (TDEA) (a.k.a. Triple DES)	*An implementation of the Data Encryption Standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than AES. (NIST SP 800-46)* *Note: Through the year 2030, TDEA and AES will coexist as FIPS-approved algorithms–thus, allowing for a gradual transition to AES.* *Also see Triple Data Encryption Standard.*
Triple Data Encryption Standard (Triple DES)	*Triple DES (i.e., TDEA) is recognized as the only FIPS-approved DES algorithm. Other implementations of the DES function are no longer authorized for protection of Federal government information. (NIST SP 800-67)* *Note: Through the year 2030, TDEA and AES will coexist as FIPS-approved algorithms–thus, allowing for a gradual transition to AES.*
Trojan Horse	*A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose. (NIST SP 800-61)*
Trusted Path	*A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can be activated only by the user or the security functions of the information system and cannot be imitated by untrusted software. (NIST SP 800-53A)*
Two-factor Authentication	*A type of authentication that requires two independent methods to establish identity and authorization to perform services. The three most recognized factors are:* • *"Something you are" (e.g., biometrics)* • *"Something you know" (e.g., password)* • *"Something you have" (e.g., smart card) (FIPS 140-3)*

Unauthorized Access	*Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use. (FIPS 191)*
Unauthorized Disclosure	*An event involving the exposure of information to entities not authorized access to the information. (NIST SP 800-57*)
Unclassified	Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. (CNSS*I 4009*)
User	(1) *Individual or (system) process authorized to access an information system. (CNSSI 4009)* (2) Any organizational or programmatic entity that [utilizes or] receives service from an [automated information system] facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or director of the facility or to the same immediate supervisor. (OMB Circular A-130)
Validation	*The process of demonstrating that the system under consideration meets in all respects the specification of that system. (FIPS 201)*
Virtual Private Network (VPN)	*(1) A virtual private network is a logical network that is established, at the application layer of the Open Systems Interconnection (OSI) model, over an existing physical network and typically does not include every node present on the physical network. (NIST SP 800-46)* *(2) A virtual network, built on top of existing physical networks, which can provide a secure communications mechanism for data and other information transmitted between networks. (NIST SP 800-113)*
Virus	*A self-replicating program that runs and spreads by modifying other programs or files (NIST SP 800-61)*
Vulnerability	*Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (FIPS 200)*
Vulnerability Assessment	*Formal description and evaluation of the vulnerabilities in an information system. (CNSSI 4009*
Warning Banner	*A notice presented prior to authentication to a access-restricted system identifying the system as a non-public resource, warning that unauthorized access can result in legal persecution and stating that only authorized users are permitted to access the system.*
Wired Equivalent Privacy (WEP)	*Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP was intended to provide the same level of security as that of a wired LAN. (NIST SP 800-46)*

Wireless Application Protocol (WAP)	*A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages. (NIST 800-48)*
Workstation	*An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. (HIPAA)*
Worm	*A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. (NIST SP 800-61)*
Write	Fundamental operation in an information system that results only in the flow of information from a subject to an object. (CNSS*I 4009*)
Write Access	Permission to write to an object in an information system. (CNSS*I 4009*)
X.509 Certificate	*The International Organization for Standardization/International Telecommunication Union – Standardization Department (ISO/ITU-T) X.509 standard defined two types of certificates – the X.509 public key certificate, and the X.509 attribute certificate. Most commonly (including this document), an X.509 certificate refers to the X.509 public key certificate. (NIST SP 800-57)*
Zeroization	*A method of erasing electronically stored data and cryptographic keys by altering or deleting the contents of the data storage to prevent recovery of the data. (Adapted from FIPS 140-2)*