Department of Health & Human Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-27
Baltimore, Maryland 21244-1850


**CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)**
Office of Information Services (OIS)
Enterprise Architecture and Strategy Group (EASG)

# CMS Information Security (IS) Acceptable Risk Safeguards (ARS)

FINAL
Version 3.1
April 24, 2008

## Summary of changes in ARS version 3.1

1. This document is available at http://www.cms.hhs.gov/informationsecurity as either a clean copy or as a markup copy enabling those individuals who were very familiar with version 3.0 of the ARS to quickly scan for and identify the substantive changes which have been made to the document in version 3.1.

2. The bulk of the changes in this version of the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) reflect revisions in the organizationally defined variables to align with CMS current processes and to correct typographical errors from version 3.0.
3. Global change – "annually" or "annual" to "every 365 days" to reflect the OMB decision on the definition of the terms.
4. Section 1, AC-2 changed to the following:,
    a. Control 0 LOW – Review information system accounts every 365 days.
    b. Control 0 MODERATE – Review information system accounts every 180 days.
    c. Control 0 HIGH – Review information system accounts every 90 days.
    d. Control 2 MODERATE and HIGH – Configure the information system to allow emergency account for a period of time Not to Exceed (NTE) 24 hours and to allow accounts with a fixed duration (i.e., temporary accounts) NTE 365 days.
    e. Control 3 LOW – Configure the information system to disable inactive accounts automatically after 365 days.
    f. Control 3 MODERATE – Configure the information system to disable inactive accounts automatically after 180 days.
    g. Control 3 HIGH – Configure the information system to disable inactive accounts automatically after 90 days.
5. Section 1, AC-7 changed to the following:
    a. Control 0 LOW – 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.
    b. Control 0 MODERATE – Configure the information systems 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 lockout to persist for a minimum of one (1) hour.
    c. Control 0 HIGH – Configure the information systems 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 lockout to persist for a minimum of three (3) hours.

6. Section 1, AC-10, Control CMS -1 changed to -- The requirement and use of more than one (1) application/process session for each user is documented in the System Security Plan.

7. Section 1, AC-11, Control 0 – changed "desktop access" to "local access".

8. Section 1, AC-12, changed to the following:
    a. Control 0 –"fifteen (15) minutes of inactivity" to "thirty (30) minutes of inactivity."
    b. Control 1 – Removed from MODERATE and retained only at the HIGH level

9. Section 3, AU-11 Control 0 – for clarity the word “audit” was added in front of “records” and “record”.

10. Section 4, CA-5 Control 0 – the update requirement for the POA&M was changed from “every three (3) months” to “monthly.”

11. Section 5, CM-7 Control 0 changed to “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. A list of specifically needed services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.”

12. Section 7, IA-4 Control 0 changed to the following:
    a. LOW – Disable user identifiers after 365 days of inactivity and delete disabled accounts during the annual recertification process.
    b. MODERATE – Same as LOW except after 180 days of inactivity.
    c. HIGH – Same as LOW except after 90 days of inactivity.

13. Section 11, PE-2 Control 0 changed to the following:
    a. LOW – Review and approve list of personnel with authorized access to facilities containing information systems at least once every 365 days.
    b. MODERATE -- Review and approve list of personnel with authorized access to facilities containing information systems at least once every 180 days.
    c. HIGH -- Review and approve list of personnel with authorized access to facilities containing information systems at least once every 90 days.

14. Section 13, PS-3, Control 0 changed to remove “Perform re-investigations once every five (5) years for sensitive positions”. OPM automatically notifies OpDivs of new criminal history entries for investigations in their file.

15. Section 13, PS-6 Control 0 changed to “Access agreements are reviewed and updated as part of the system accreditation or when a contract is renewed or extended.”

16. Section 14, RA-5 Control 0 changed “quarterly” to “90 days.”

17. Section 16, SC-5 Control 0 – added URLs for the SANS and NIST references.

18. Section 16, SC-9 Control 1 – added (see SC-CMS-4 for E-mail).

19. Section 16, SC-CMS-4 Control CMS-1 – removed: HIGH CMS-0 control changed to “Same as Moderate.”

20. Section 17, SI 6 Control 0 and 1 – MOVE to HIGH only and state “Not Required” under MODERATE.

21. Section 17, SI-7 changed to the following:

a. Control CMS-1 removed.
b. "Not Required" inserted for LOW.
c. Control 1 – Removed from MODERATE and HIGH language changed to "Perform weekly integrity scans of the system."
d. Control CMS-2 moved to Section 16, SA-11.

## Summary of changes in ARS version 3.0

1. This document is available at http://www.cms.hhs.gov/informationsecurity as either a clean copy or as a markup copy enabling those individuals who were very familiar with version 2.0 of the ARS to quickly scan for and identify the substantive changes which have been made to the document in version 3.0.

2. The bulk of the changes in this version of the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) reflect the new standards to which CMS must comply as established by the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 1, Recommended Security Controls for Federal Information Systems*, dated December 2006. Additional changes have been made in order to comply with new directives and guidance from the Office of Management and Budget, (OMB), the Department of Health and Human Services (DHHS) and industry best practices.

3. Global change – "System Owner" is now "Business Owner"

4. Global change – "service category" is now "control family".

5. References to "ARS Category" changed to "ARS Family" for all ARS 3.0 references.

6. The introductory text at the beginning of each control family has been aligned to the definitions for the 17 security-related areas in the *Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems*, dated March 9, 2006.

7. The appendices have been rearranged for ease of use.

    a. Appendix A, Standards Category Classification has been moved to Appendix B and renamed "Standards Family Classification".
    b. Appendix B, Standards Redistribution, has been moved to Appendix C and renamed Historical Log of ARS Standards Redistribution.
    c. Appendix C, E-Authentication, has been moved to Appendix A, and renamed E-Authentication Standards

8. Appendix A, E-Authentication Standards, was updated for clarity and to reflect the new standards to which CMS must comply as established by changes to *NIST SP 800-63, Electronic Authentication Guideline v1.0.2*, dated April 2006

9. Table 1 is a listing of the new control numbers in each control family in the CMS ARS based on the new requirements of NIST SP 800-53 Rev 1 controls.

**Table 1: New ARS 3.0 Standards based on NIST 800-53 Rev 1 by Family**

| ARS No. | ARS Standard |
|---|---|
| ***ARS Family:*** | ***Access Control (AC)*** |
| AC-12.1 | Session Termination |
| AC-17.4 | Remote Access |
| AC-18.1 | Wireless Access Restrictions |
| AC-18.2 | Wireless Access Restrictions |
| AC-20.1 | Use of External Information Systems |
| ***ARS Family:*** | ***Awareness and Training (AT)*** |
| AT-5 | Contacts with Security Groups and Associations |
| ***ARS Family:*** | ***Audit and Accountability (AU)*** |
| AU-2.3 | Auditable Events |
| AU-5.1 | Response to Audit Processing Failures |
| AU-5.2 | Response to Audit Processing Failures |
| AU-7.1 | Audit Reduction and Report Generation |
| AU-8.1 | Time Stamps |
| ***ARS Family:*** | ***Certification, Accreditation, and Security Assessments (CA)*** |
| CA-4.1 | Security Certification |
| CA-5.CMS-1 | Plan of Action and Milestones |
| CA-7.1 | Continuous Monitoring |
| ***ARS Family:*** | ***Configuration Management (CM)*** |
| CM-5 | Access Restrictions for Change |
| CM-8 | Information System Component Inventory |
| CM-8.1 | Information System Component Inventory |
| CM-8.2 | Information System Component Inventory |
| ***ARS Family:*** | ***Contingency Planning (CP)*** |
| CP-2.2 | Contingency Plan |
| CP-9.4 | Information System Backup |
| ***ARS Family:*** | ***Identification and Authentication (IA)*** |
| IA-2.2 | User Identification and Authentication |
| IA-2.3 | User Identification and Authentication |
| IA-2.CMS-3 | User Identification and Authentication |
| ***ARS Family:*** | ***Media Protection (MP)*** |
| MP-5.1 | Media Transport |
| MP-5.2 | Media Transport |
| MP-5.3 | Media Transport |
| ***ARS Family:*** | ***Physical and Environmental Protection (PE)*** |
| PE-3.1 | Physical Access Control |
| PE-4.CMS-2 | Access Control for Transmission Media |
| PE-8.2 | Access Records |
| PE-9.CMS-2 | Power Equipment and Cabling |

| ARS No. | ARS Standard |
|---|---|
| PE-18 | Location of Information System Components |
| PE-18.1 | Location of Information System Components |
| PE-19 | Information Leakage |
| ***ARS Family:*** | ***Planning (PL)*** |
| PL-6 | Security-Related Activity Planning |
| ***ARS Family:*** | ***System and Services Acquisition (SA)*** |
| SA-4.1 | Acquisitions |
| SA-4.2 | Acquisitions |
| ***ARS Family:*** | ***System and Communications Protection (SC)*** |
| SC-7.2 | Boundary Protection |
| SC-7.3 | Boundary Protection |
| SC-7.4 | Boundary Protection |
| SC-20 | Secure Name /Address Resolution Service (Authoritative Source) |
| SC-20.1 | Secure Name /Address Resolution Service (Authoritative Source) |
| SC-21 | Secure Name /Address Resolution Service (Recursive or Caching Resolver) |
| SC-21.1 | Secure Name /Address Resolution Service (Recursive or Caching Resolver) |
| SC-22 | Architecture and Provisioning for Name /Address Resolution Service |
| SC-23 | Session Authenticity |
| ***ARS Family:*** | ***System and Information Integrity (SI)*** |
| SI-4.5 | Information System Monitoring Tools and Techniques |
| SI-7.1 | Software and Information Integrity |
| SI-7.2 | Software and Information Integrity |
| SI-7.3 | Software and Information Integrity |

10. Table 2 lists the new CMS standards which are not based on NIST SP 800-53 Rev 1 controls and their source.

**Table 2: New ARS 3.0 Standards <u>not</u> based on NIST 800-53 Rev 1 by Category**

| ARS No. | ARS Standard | Source |
|---|---|---|
| ***ARS Family:*** | ***Access Control (AC)*** | ***Access Control (AC)*** |
| AC-CMS-1 | System Boot Access | Industry Best Practices |
| ***ARS Family:*** | ***Maintenance (MA)*** | ***Maintenance (MA)*** |
| MA-CMS-1 | Off-site Physical Repair of Systems | • Industry Best Practices<br>• *NIST SP 800-64 Integrating Security into the System Development Life-Cycle (SDLC)* |
| MA-CMS-2 | On-site Physical Repair of Systems | • Industry Best Practices<br>• *NIST SP 800-64 Integrating Security into the SDLC* |

| ***ARS Family:*** | ***Media Protection (MP)*** | ***Media Protection (MP)*** |
|---|---|---|
| MP-CMS-1 | Media Related Records | Industry Best Practices |
| ***ARS Family:*** | ***Personnel Security (PS)*** | ***Personnel Security (PS)*** |
| PS-CMS-1 | Review System Access During Extraordinary Personnel Circumstances | • Industry Best Practices<br>• *CMS Master Security Plan*<br>• *CMS Business Partners Systems Security Manual (BPSSM)* |
| PS-CMS-2 | Designate an Information System Security Officer (ISSO) / System Security Officer (SSO) | • Industry Best Practices<br>• CMS Handbook |
| ***ARS Family:*** | ***System and Communications Protection (SC)*** | ***System and Communications Protection (SC)*** |
| SC-CMS-1 | Desktop Modems | • Industry Best Practices<br>• CMS Master Security Plan<br>• *CMS BPSSM* |
| SC-CMS-2 | Identify and Detect Unauthorized Modems | Industry Best Practices |
| SC-CMS-3 | Secondary Authentication and Encryption | Industry Best Practices |
| SC-CMS-4 | Electronic Mail | • Industry Best Practices<br>• *CMS Master Security Plan* |
| SC-CMS-5 | Persistent Cookies | Industry Best Practices |
| SC-CMS-6 | Network Interconnection | Industry Best Practices |

11. Table 3 lists those former ARS standards which have been removed as a CMS standard and have been replaced by a NIST SP 800-53 Rev 1 control.

**Table 3: Former ARS 2.0 Non-NIST 800-53 Standards by Category**

| ARS No. | ARS Standard | Disposition |
|---|---|---|
| ***ARS Family:*** | ***Certification, Accreditation, and Security Assessments (CA)*** | ***Certification, Accreditation, and Security Assessments (CA)*** |
| CA-CMS-1 | Information Sensitivity Assessment | Controls consolidated with RA-3 |
| ***ARS Family:*** | ***Identification and Authentication (IA)*** | ***Identification and Authentication (IA)*** |
| IA-CMS-1 | Help Desk Support Procedures | Controls moved to IA-2.CMS-3 |
| ***ARS Family:*** | ***Physical and Environmental Protection (PE)*** | ***Physical and Environmental Protection (PE)*** |
| PE-CMS-1 | Power Surge Protection | Controls moved to PE-9.CMS-2 |
| PE-CMS-2 | Physical Ports | Controls moved to PE-4.CMS-2 |

| | | |
|---|---|---|
| PE-CMS-3 | Restrict the Use of Portable Computing Devices (formerly Handheld Personal Computers) | Controls deleted as they are included in AC-19 |

12. ARS standard CP-CMS-1 has been removed as it is now covered in current CMS CP Procedures.

## Summary of changes in ARS version 2.0

Items 1 through 5, below, reflect the changes in the Centers for Medicare & Medicaid Services (CMS) requirements to comply with the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems*, dated February 2005 (includes updates through 05-04-2005).

1. The following categories and/or standards within the Acceptable Risk Safeguards (ARS) version 1.2 were removed and replaced by policy statements within the CMS Policy for the Information Security Program, dated May 2005:
   a. Certification and Accreditation Standards
      i. 5.1 – Assign Responsibility for Security within Each System
   b. System Access Security Standards
      i. 7.22 – User Access Administration

2. Numerous standards were added to ARS 2.0 to further comply with NIST SP 800-53 (controls and guidance) and to adhere to the Department of Health and Human Services (DHHS) policies and guidance. CMS has adopted additional standards based on CMS Policies, Procedures and Guidance; other Federal and non-Federal guidance resources and industry best practices. Table 4 lists those standards and their sources.

**Table 4: ARS 2.0 Non-NIST 800-53 Standards by Category**

| Proposed ARS No. | Proposed ARS Standard | Source |
|---|---|---|
| ***Proposed ARS Category:*** | ***Access Control (AC)*** | ***Access Control (AC)*** |
| AC-CMS-1 | System Boot Access | Industry Best Practices |
| ***Proposed ARS Category:*** | ***Certification, Accreditation, and Security Assessments (CA)*** | ***Certification, Accreditation, and Security Assessments (CA)*** |
| CA-CMS-1 | Information Sensitivity Assessment | • Industry Best Practices<br>• *CMS Information System (IS) Risk Assessment (RA) Methodology*<br>• *FIPS 199* |
| ***Proposed ARS Category:*** | ***Contingency Planning (CP)*** | ***Contingency Planning (CP)*** |
| CP-CMS-1 | Disaster Recovery Plan | • Industry Best Practices<br>• *CMS Master Security Plan*<br>• FISMA |
| ***Proposed ARS*** | ***Identification and Authentication (IA)*** | ***Identification and Authentication (IA)*** |

| Proposed ARS No. | Proposed ARS Standard | Source |
|---|---|---|
| ***Category:*** | | |
| IA-CMS-1 | Help Desk Support Procedures | • Industry Best Practices<br>• *CMS Enterprise Password Standard*<br>FISMA |
| ***Proposed ARS Category:*** | ***Maintenance (MA)*** | ***Maintenance (MA)*** |
| MA-CMS-1 | Off-site Physical Repair of Systems | • Industry Best Practices<br>• *NIST SP 800-64 Integrating Security into the System Development Life-Cycle (SDLC)* |
| MA-CMS-2 | On-site Physical Repair of Systems | • Industry Best Practices<br>• *NIST SP 800-64 Integrating Security into the SDLC* |
| ***Proposed ARS Category:*** | ***Media Protection (MP)*** | ***Media Protection (MP)*** |
| MP-CMS-1 | Media Related Records | *NIST SP 800-53, Second Public Draft* |
| ***Proposed ARS Category:*** | ***Physical and Environmental Protection (PE)*** | ***Physical and Environmental Protection (PE)*** |
| PE-CMS-1 | Power Surge Protection | • Industry Best Practices<br>• *CMS Master Security Plan* |
| PE-CMS-2 | Environmental Controls | Industry Best Practices |
| PE-CMS-3 | Physical Ports | Industry Best Practices |
| PE-CMS-4 | Restrict the Use of Portable Computing Devices (formerly Handheld Personal Computers) | Industry Best Practices |
| ***Proposed ARS Category:*** | ***Personnel Security (PS)*** | ***Personnel Security (PS)*** |
| PS-CMS-1 | Review System Access During Extraordinary Personnel Circumstances | • Industry Best Practices<br>• *CMS Master Security Plan*<br>• *CMS Business Partners Systems Security Manual (BPSSM) core set of security requirements (CSR) 1.1.9* |
| PS-CMS-2 | Designate an Information System Security Officer (ISSO) / System Security Officer (SSO) | • Industry Best Practices<br>• CMS Handbook |
| PS-CMS-3 | Data Ownership and Stewardship | Industry Best Practices |

| Proposed ARS No. | Proposed ARS Standard | Source |
|---|---|---|
| ***Proposed ARS Category:*** | ***System and Communications Protection (SC)*** | ***System and Communications Protection (SC)*** |
| SC-CMS-1 | Desktop Modems | • Industry Best Practices<br>• CMS Master Security Plan<br>• *CMS BPSSM* |
| SC-CMS-2 | Identify and Detect Unauthorized Modems | Industry Best Practices |
| SC-CMS-3 | Secondary Authentication and Encryption | Industry Best Practices |
| SC-CMS-4 | Electronic Mail | • Industry Best Practices<br>• *CMS Master Security Plan* |
| SC-CMS-5 | Persistent Cookies | Industry Best Practices |

3. Appendix A, *CMS Acceptable Risk Safeguards for e-Authentication*, has been added based on NIST SP 800-63 V1.0.1, *Electronic Authentication Guideline*, dated September 2004.

    a. There will be recurring old ARS standards within different categories, due to the applicability of their parts. In cases where standards recur, only the specific portions of the standard, which apply, are included within the new standard.

    b. The old ARS standards are listed in ascending order, within each category, for tracking purposes

4. The standards from the ARS, version 1.2, are redistributed throughout the new categories of this proposed ARS. The table within Appendix B, Historical Log of ARS Standards Redistribution, maps the old standards to their new name and location.

5. An explanation of the numbering scheme for the various controls was added. See the "STANDARDS NUMBERING SCHEMA".

## Summary of changes in ARS version 1.2

Items below reflect the changes in ARS version 1.2 from the original version.

1. Section 3.2, [Organizational Practice Security Standards column] "Information Sensitivity Assessment" (ISA) change to "CMS Information Security Business Risk Assessment (RA)".
2. Section 3.2, Low, Moderate and High, change "an ISA" to "a Business RA".
3. Section 3.2, Low, Moderate and High, remove "Section 10.5 of the".

4. Section 3.4, Low, Moderate and High, add “or equivalent,” following “management procedures,”.
5. Section 3.14, Low, Moderate and High, add “and/or CMS SSP Methodology.” following “CMS Roadmap”.
6. Section 4.6, [Security Management Standards column], add “/System Security Officer (SSO)” following “(ISSO)”.
7. Section 4.6, Low, Moderate and High, add “/SSO” following “ISSO”.
8. Section 6.2, Low, Moderate and High, add “external communications” after “All”.
9. Section 7.3, Low and High, replace in its entirety with “Configure operating system controls to disable public read and write access to files, objects, and directories that may directly impact system functionality or performance, or that contain sensitive information.
10. Section 7.18, Moderate and High, add “highly” after “Encrypt”.
11. Section 8.2, Moderate and High, replace in its entirety with “Implement technical security measures to guard against unauthorized access to sensitive information that is being transmitted over an electronic communications network.”
12. Section 9.1, Moderate, add “and must be encrypted when residing in non-secure areas.” after “controls.”
13. Section 9.1, High, add “when residing in non-secure areas.” after “encrypted.”
14. Section 9.9, High, change “every other day” to “weekly”.

Section 10.6, Low, Moderate and High, add “once an incident has occurred” after “forensic evidence”.

# Table of Contents

# INTRODUCTION

The ARS contains a broad set of required security standards based upon *NIST SP 800-53Revision 1, Recommended Security Controls for Federal Information Systems*, dated December 2006, and *NIST 800-63 Version 1.0.2, Electronic Authentication Guideline*, dated, April 2006 as well as additional standards based on CMS Policies, Procedures, and Guidance, other Federal and non-Federal guidance resources and industry leading security practices. This document provides technical guidance to CMS and its contractors as to the *minimum* level of security controls that must be implemented to protect CMS' information and information systems.

Incorporating controls required by this document will ensure that all CMS systems meet a minimum level of information security. However, many CMS systems, particularly those that are mission-critical or that are available to Internet users, will require additional security protections.[1] A system may be required to meet additional, higher-level or more rigorous, information protection requirements as mandated by specific federal, legal, program, or accounting sources. For example, section 3, Audit and Accountability, states that for systems with a HIGH system security level, the logs will be retained for ninety (90) days and then archived for one (1) year. However, the National Archives and Records Administration has determined that Audit Files (NC1-440-78-1, Item B) be retained for four (4) years after completion of the audit. The CMS system must be developed to meet these higher-level standards where applicable. **The CMS ARS shall not be construed to relieve or waive these other standards.**

It is important to note that the ARS does not address either specific business process requirements or the full suite of internal controls that together ensure that business requirements are fulfilled. The goal of the ARS is to provide a baseline of minimally acceptable internal controls that pertain to information security. It is the responsibility of the Business Owner of CMS systems, in collaboration with the Office of Information Services (OIS), to ensure that all business process-related internal controls are incorporated into CMS systems. Business Owners must document and certify the incorporated security / internal controls in the CMS Information Security (IS) Risk Assessment (RA) and/or CMS System Security Plan (SSP) for the system.

# PURPOSE

All federal systems must incorporate IS controls to protect federal information assets. These controls cover areas of security ranging from the physical environment to auditing and logging. CMS developed the ARS, utilizing the NIST SP 800-53 (as amended) as the primary resource to categorize the controls. The purpose of the ARS is to define information security minimum

[1] For example, CMS has published the CMS Internet Architecture document to describe architectures and standards that must be in place for Internet-facing systems. Business Owners should refer to the following web site: http://www.cms.hhs.gov/SystemLifecycleFramework/09_Standards.asp#TopOfPage to ensure that all CMS information security requirements are met.

requirements for CMS systems based on the system's designated system security level. (See *CMS Information Security Levels* at: http://www.cms.hhs.gov/InformationSecurity/14_standards.asp#TopOfPage.) Appendix A, addresses e-Authentication Standards, for web-based applications. These standards provide the means with which to make transactions for individuals requiring additional security assurances.

The ARS complies 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. It is not intended to be an all-inclusive list of security controls and is subject to regular updates to reflect the changing technological environment. The ARS is not intended to replace a Business Owner's due diligence to incorporate controls to mitigate risk. These controls must be considered throughout the risk management process and the System Development Life Cycle (SDLC), and employed when appropriate and feasible.

The Business Owner and system developer / maintainer are the target audience for the ARS. They have primary responsibility for determining the information security requirements and ensuring their implementation. However, any entity involved in the SDLC could use this information to understand the baseline information security protections required by CMS. For additional information on how the ARS integrates into the CMS system security life-cycle, refer to http://www.cms.hhs.gov/informationsecurity.

# STANDARDS NUMBERING SCHEMA

This CMS ARS is divided into seventeen (17) security control families as established by the NIST SP 800-53 which are aligned closely with the 17 security-related areas specified in *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*:

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Certification, Accreditation, and Security Assessments (CA)
5. Configuration Management (CM)
6. Contingency Planning (CP)
7. Identification and Authentication (IA)
8. Incident Response (IR)
9. Maintenance (MA)
10. Media Protection (MP)
11. Physical and Environmental Protection (PE)
12. Planning (PL)
13. Personnel Security (PS)
14. Risk Assessment (RA)
15. System and Services Acquisition (SA)
16. System and Communications Protection (SC)
17. System and Information Integrity (SI)

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

Safeguards are presented by control family with each numbered row indicating a base control (the terms safeguard and control are synonymous in this context). NIST SP 800-53 Rev. 1 numbering scheme is used, i.e., the security control family acronym followed by a sequential number, e.g., AC-1, AC-2, etc. Each row has an ARS standards column, and columns pertaining to "Low", "Moderate", and "High" security levels. The ARS "Standards" column contains the base control number and name, and the cross reference to the appropriate PISP policy that defines the underlying base control. All referenced PISP policies are required, unless specifically stated as "Not required." for a security level.

Some controls may have required enhancements or amplifications. These are identified in the applicable security level columns labeled: "Low", "Moderate", and "High" for each row. The NIST SP 800-53 Rev. 1 numbering scheme is used to designate enhancements, e.g., a sequential number starting at 1 for each base control. An enhancement numbered "0" is used when amplification or defining of periodicity of controls indicated in the underlying PISP policy statement is required.

While most controls map directly to prescribed Federal minimum standards (defined in the NIST SP 800-53), there are additional controls and enhancements unique to CMS. These are distinguished by the characters "CMS-" followed by a sequential number in the base control and / or enhancement. Thus, AC-2(CMS-1) is the first CMS unique enhancement to control AC-2, and AC-CMS-1 is the first CMS unique base control in the Access Control (AC) family.

# HOW TO USE THIS DOCUMENT

First, the Business Owner needs to determine the system's system security level based on the *CMS Information Security Levels* (http://www.cms.hhs.gov/InformationSecurity/14_standards.asp#TopOfPage), or the sensitivity level of the position for Personnel Security (PS) based on the 5 CFR 731.106(a) and Office of Personnel Management (OPM) policy and guidance. Since the ARS controls are represented by system security level or position sensitivity level, the required controls for a particular system will be based on the applicable designation level.

The controls within the ARS that may apply will depend on the scope 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).

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 ARS and determining the appropriateness for their system.

**NOTE:**
1) All CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions shall observe the individual policy statements described in CMS PISP. Unless an ARS control is stated as "Not Required" or otherwise noted in the ARS control, the control standards included in the ARS are in addition to the security policies and controls described in the CMS PISP.

2) These standards are the minimum thresholds for the various controls defined in the ARS. A Business Owner may choose to strengthen the controls ensuring the best possible protection of CMS information and information systems.

3) Sometimes controls 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 must be considered as part of risk management and the alternative or compensating controls must be documented in the IS RA and SSP, and approved by the Chief Information Officer (CIO) or his/her designated representative.

4) In Appendix A, *CMS Acceptable Risk Safeguards for e-Authentication*, assurance levels differ from the CMS HIGH, MODERATE, and LOW system security levels. Refer to the Appendix A for details.

# 1. ACCESS CONTROL (AC)

The standards listed in this section focus on how the organization must 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.

**NOTE:** When a control for a system is subject to higher standards to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **AC-1**<br>**Access Control Policy and Procedures**<br>***PISP Sec. 4.1.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **AC-2**<br>**Account Management**<br>***PISP Sec. 4.1.2*** | 0 – Review information system accounts every 365 days and require annual certification.<br><br>3 – Configure the information system to disable inactive accounts automatically after 365 days.<br><br>CMS-1 – Remove or disable default user accounts. Rename active default accounts. | 0 – Review information system accounts every 180 days and require annual certification.<br><br>1 – Employ automated mechanisms to support the management of information system accounts.<br><br>2 – Configure the information system to allow emergency account for a period of time NTE | 0 – Review information system accounts every 90 days and require annual certification.<br><br>1 thru 2 – Same as Moderate.<br><br>3 – Configure the information system to disable inactive accounts automatically after 90 days.<br><br>4 – Same as Moderate. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | CMS-2 – Require the use of unique and separate administrator accounts for administrator and non-administrator activities.<br><br>CMS-3 – Implement centralized control of user access administrator functions.<br><br>CMS-4 – Regulate the access provided to contractors and define security requirements for contractors.<br><br>CMS-5 – Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination. | 24 hours and to allow accounts with a fixed duration (i.e., temporary accounts) NTE 365 days.<br><br>3 – Configure the information system to disable inactive accounts automatically after 180 days.<br><br>4 – 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.<br><br>CMS-1 thru CMS-4 – Same as Low.<br><br>CMS-5 – 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. | CMS-1 thru CMS-4 – Same as Low.<br><br>CMS-5 – Same as Moderate. |
| **AC-3** | 1 – Ensure the information system | 1 – Same as Low. | 1 – Same as Low. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Access Enforcement**<br><br>***PISP Sec. 4.1.3*** | 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.<br><br>CMS-1 – 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).<br><br>CMS-2 – If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix A for *e-Authentication Standards*.<br><br>CMS-3 – Configure operating system controls to disable public "write" access to files, objects, and directories that may directly impact system functionality and/or | CMS-1 thru CMS-2 – Same as Low.<br><br>CMS-3 – 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.<br><br>CMS-4 – Data stored in the information system must be protected with system access controls. | CMS-1 thru CMS-2 – Same as Low.<br><br>CMS-3 – 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.<br><br>CMS-4 – Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | performance. | | |
| **AC-4**<br>**Information Flow Enforcement**<br>***PISP Sec. 4.1.4*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **AC-5**<br>**Separation of Duties**<br>***PISP Sec. 4.1.5*** | CMS-1 – Ensure that audit functions are not performed by security personnel responsible for administering access control.<br><br>CMS-2 – Maintain a limited group of administrators with access based upon the users' roles and responsibilities.<br><br>CMS-3 – Ensure that critical mission functions and information system support functions are divided among separate individuals.<br><br>CMS-4 – Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided | CMS-1 thru CMS-4 – Same as Low.<br><br>CMS-5 – 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. | CMS-1 thru CMS-4 – Same as Low.<br><br>CMS-5 – Same as Moderate.<br><br>CMS-6 – 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. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | among separate individuals or groups. | | |
| **AC-6**<br>**Least Privilege**<br>***PISP Sec. 4.1.6*** | CMS-1 – Disable all file system access not explicitly required for system, application, and administrator functionality.<br><br>CMS-2 – 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.<br><br>CMS-3 – Restrict the use of database management utilities to only authorized database administrators. | CMS-1 thru CMS-2 – Same as Low.<br><br>CMS-3 – 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.<br><br>CMS-4 – 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. | CMS-1, CMS-2 – Same as Low.<br><br>CMS-3 – 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.<br><br>CMS-4 – Same as Moderate. |
| **AC-7**<br>**Unsuccessful Log-on** | 0 – Configure the information system to disable access for at least five (5) minutes after three (3) failed log-on attempts by a | 0 – Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user during a | 0 – Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Attempts**<br><br>***PISP Sec. 4.1.7*** | user during a five (5) minute time period. | fifteen (15) minute time period. Require the lock out to persist for a minimum of one (1) hour. | user during a one (1) hour time period. Require the lock out to persist for a minimum of three (3) hours. |
| **AC-8**<br>**System Use Notification**<br><br>***PISP Sec. 4.1.8*** | CMS-1 – Configure the information system to display a warning banner automatically prior to granting access to potential users. Notify users that:<br>(a) They are accessing a U.S. Government information system;<br>(b) CMS maintains ownership and responsibility for its computer systems;<br>(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;<br>(d) Their usage may be monitored, recorded, and audited;<br>(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and<br>(f) The use of the information system establishes their consent to any and all | CMS-1 thru CMS-3 – Same as Low. | CMS-1 thru CMS-3 – Same as Low. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | monitoring and recording of their activities.<br><br>CMS-2 – Develop and implement the warning banner in conjunction with legal counsel.<br><br>CMS-3 – 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. | | |
| **AC-9**<br>**Previous Log-on Notification**<br><br>***PISP Sec. 4.1.9*** | Not required. | Not required. | 0 – 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. |
| **AC-10**<br>**Concurrent Session Control**<br><br>***PISP Sec. 4.1.10*** | Not required. | 0 – 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. | 0 – Same as Moderate.<br><br>CMS-1 – Same as Moderate. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | CMS-1 – The requirement and use of more than one (1) application/process session for each user is documented in the SSP. | |
| **AC-11**<br>**Session Lock**<br>***PISP Sec. 4.1.11*** | Not required. | 0 – 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. | 0 – Same as Moderate. |
| **AC-12**<br>**Session Termination**<br>***PISP Sec. 4.1.12*** | Not required. | 0 – Configure the information system to automatically terminate all remote sessions (user and information system) after 30 minutes of inactivity. | 0 – Same as Moderate.<br>1 – Automatic session termination applies to local and remote sessions. |
| **AC-13**<br>**Supervision and Review – Access Control**<br>***PISP Sec. 4.1.13*** | CMS-1 – 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 | 1 – Employ automated mechanisms to facilitate the review of user activities.<br>CMS-1 – Same as Low.<br>CMS-2 – Enable logging of | 1 – Same as Moderate.<br>CMS-1 – Same as Low.<br>CMS-2 – Same as Moderate.<br>CMS-3 – Inspect administrator |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | alert notification for technical staff review and assessment.<br><br>CMS-2 – Enable logging of administrator and user account activities, system shutdowns, reboots, errors and access authorizations.<br><br>CMS-3 – 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. | administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations.<br><br>CMS-3 – 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. | 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. |
| **AC-14**<br>**Permitted Actions without Identification or Authentication**<br><br>***PISP Sec. 4.1.14*** | No additional controls required beyond the referenced policy. | 0 – Identify and document specific user actions that can be performed on the information system without identification or authentication.<br><br>1 – 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. | 0, 1 – Same as Moderate. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **AC-15**<br>**Automated Marking**<br>***PISP Sec. 4.1.15*** | Not required. | Not required. | No additional controls required beyond the referenced policy. |
| **AC-16**<br>**Automated Labeling**<br>***PISP Sec. 4.1.16*** | CMS-1 – 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). | CMS-1 – Same as Low. | CMS-1 – Same as Low. |
| **AC-17**<br>**Remote Access**<br>***PISP Sec. 4.1.17*** | 1 thru 3 – Not required.<br><br>4 – 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.<br><br>CMS-1 – Enable secure management protocols through a VPN link(s) if connected to the information system and using remote administration. | 1 – Employ automated mechanisms to facilitate the monitoring and control of remote access methods.<br><br>2 – Employ cryptography to protect the confidentiality and integrity of remote access sessions.<br><br>3 – Control all remote access through a limited number of managed access control points.<br><br>4 – Same as Low. | 1 thru 3 – Same as Moderate.<br><br>4 – Same as Low.<br><br>CMS-1 – Same as Moderate<br><br>CMS-2 – Same as Low.<br><br>CMS-3 – Require callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | CMS-2 – Implement password protection for remote access connections.<br><br>CMS-3 – Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) cannot be used.<br><br>CMS-4 – If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix A for e-Authentication standards. | CMS-1 – 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).<br><br>CMS-2 thru CMS-4 – Same as Low. | 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.<br><br>CMS-4 – Same as Low. |
| **AC-18**<br>**Wireless Access Restrictions**<br><br>***PISP Sec. 4.1.18*** | 0 – CMS policy prohibits the use of wireless access unless explicitly approved by the CMS CIO or his/her designated representative. | 0 – Same as Low.<br><br>1 – If wireless access is explicitly approved, approved authentication and encryption is used to protect wireless access to the information system.<br><br>2 – Perform quarterly scans for unauthorized wireless access | 0 – Same as Low.<br><br>1, 2 – Same as Moderate. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | points and take appropriate action if any access points are discovered. | |
| **AC-19**<br>**Access Control for Portable and Mobile Devices**<br>***PISP Sec. 4.1.19*** | No additional controls required beyond the referenced policy. | CMS-1 – 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:<br>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. | CMS-1 – Same as Moderate. |
| **AC-20**<br>**Use of External Information Systems**<br>***PISP Sec. 4.1.20*** | CMS-1 – Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal | 1 – Users are prohibited from using any external information system to access the information system or to process, store, or transmit CMS-controlled | 1 – Same as Moderate.<br><br>CMS-1 – Same as Low. |

| Access Control (AC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | 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. | information except in situations where the organization:<br>(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<br>(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.<br><br>CMS-1 – Same as Low. | |
| **AC-CMS-1**<br>**System Boot Access**<br>***PISP Sec. 4.1.21***<br><br>***Best Practice*** | CMS-1 – If not explicitly required, boot access to removable media drives is disabled.<br><br>CMS-2 – System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management). | CMS-1, CMS-2 – Same as Low.<br><br>CMS-3 – If not explicitly required, removable media drive functionality is disabled. | CMS-1, CMS-2 – Same as Low.<br><br>CMS-3 – Same as Moderate. |

## 2. AWARENESS AND TRAINING (AT)

The standards listed in this section focus on how the organization must: (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.

**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Awareness and Training (AT) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **AT-1**<br>**Security Awareness and Training Policy and Procedures**<br>***PISP Sec. 4.2.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **AT-2**<br>**Security Awareness**<br>***PISP Sec. 4.2.2*** | 0 – 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 | 0 – Same as Low.<br><br>CMS-1 – Same as Low. | 0 – Same as Low.<br><br>CMS-1 – Same as Low. |

| Awareness and Training (AT) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | every 365 days thereafter.<br><br>CMS-1 – Establish a program to promote continuing awareness of information security issues and threats. | | |
| **AT-3**<br>**Security Training**<br><br>***PISP Sec. 4.2.3*** | 0 – 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. | 0 – Same as Low. | 0 – Same as Low. |
| **AT-4**<br>**Security Training Records**<br><br>***PISP Sec. 4.2.4*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **AT-5**<br>**Contacts with** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

| Awareness and Training (AT) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Security Groups and Associations**<br><br>***PISP Sec. 4.2.5*** | | | |

# 3. AUDIT AND ACCOUNTABILITY (AU)

The standards listed in this section focus on how the organization must: (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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| **Audit and Accountability (AU) Standards** | **System Security Level Low** | **System Security Level Moderate** | **System Security Level High** |
|---|---|---|---|
| **AU-1**<br>**Audit and Accountability Policy and Procedures**<br>***PISP Sec. 4.3.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **AU-2**<br>**Auditable Events**<br>***PISP Sec. 4.3.2*** | 0 – Generate audit records for the following events:<br>(a) User account management activities,<br>(b) System shutdown,<br>(c) System reboot,<br>(d) System errors,<br>(e) Application shutdown,<br>(f) Application restart,<br>(g) Application errors, | 0 – Same as Low except generate audit records for the following **additional** events:<br>(j) File modification,<br>(k) Failed and successful log-ons,<br>(l) Security policy modifications, and<br>(m) Use of administrator privileges. | 0 – Same as Moderate except generate audit records for the following **additional** events:<br>(n) File access.<br><br>1, 2, 3 – Same as Moderate.<br><br>CMS-1 – Same as Moderate.<br><br>CMS-2 – Same as Low. |

| Audit and Accountability (AU) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | (h) File creation, and<br>(i) File deletion.<br>CMS-1 – Enable logging-on for perimeter devices, including firewalls and routers.<br>(a) Log packet screening denials originating from untrusted networks,<br>(b) packet screening denials originating from trusted networks,<br>(c) user account management,<br>(d) modification of packet filters,<br>(e) application errors,<br>(f) system shutdown and reboot, and<br>(g) system errors.<br><br>CMS-2 – Verify that proper logging is enabled in order to audit administrator activities. | 1 – Provide the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical) time correlated audit trail.<br><br>2 – Provide the capability to manage the selection of events to be audited by individual components of the information system.<br><br>3 – Periodically review and update the list of auditable events.<br><br>CMS-1 – Enable logging for perimeter devices, including firewalls and routers.<br>(a) Log packet screening denials originating from un-trusted networks,<br>(b) packet screening denials originating from trusted networks,<br>(c) user account management, | |

| Audit and Accountability (AU) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | (d) modification of proxy services,<br>(e) application errors,<br>(f) system shutdown and reboot,<br>(g) system errors,<br>(h) modification of proxy services, and<br>(i) modification of packet filters.<br><br>CMS-2 – Same as Low. | |
| **AU-3**<br>**Content of Audit Records**<br><br>***PISP Sec. 4.3.3*** | No additional controls required beyond the referenced policy. | 1 – Provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.<br><br>CMS-1 – 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. | 1 – Same as Moderate.<br><br>2 – Centrally manage the content of audit records generated by individual components throughout the system.<br><br>CMS-1 – Same as Moderate. |
| **AU-4**<br>**Audit Storage** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

| Audit and Accountability (AU) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Capacity**<br><br>***PISP Sec. 4.3.4*** | | | |
| **AU-5**<br>**Response to Audit Processing Failures**<br><br>***PISP Sec. 4.3.5*** | 0 – Alert appropriate officials and take the following actions in response to an audit failure or audit storage capacity issue:<br>(a) Shutdown the information system,<br>(b) Stop generating audit records, or<br>(c) Overwrite the oldest records, in the case that storage media is unavailable. | 0 – Same as Low. | 0 – Same as Low.<br><br>1 – The information system provides a warning when allocated audit record storage volume reaches 80% of audit record storage capacity.<br><br>2 – A second real-time alert is sent when the audit record log is full. |
| **AU-6**<br>**Audit Monitoring, Analysis, and Reporting**<br><br>***PISP Sec. 4.3.6*** | CMS-1 – 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.<br><br>CMS-2 – Review network traffic, | 1 – Employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.<br><br>2 – Employ automated mechanisms to immediately alert security personnel of the following minimal examples of inappropriate or unusual activities with security | 1, 2 – Same as Moderate.<br><br>CMS-1 thru CMS-3 – Same as Low.<br><br>CMS-4 – Use automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.<br><br>CMS-5 – Inspect administrator groups on demand but at least |

| Audit and Accountability (AU) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | 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.<br><br>CMS-3 – Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.<br><br>CMS-4 – Use automated utilities to review audit records at least once every fourteen (14) days for unusual, unexpected, or suspicious behavior.<br><br>CMS-5 – Inspect administrator groups on demand but no less than once every thirty (30) days to ensure unauthorized administrator accounts have not been created. | implications: threats to infrastructure, systems or assets; threats to CMS sensitive data; and threats to finances, personnel, or property.<br><br>CMS-1 thru CMS-3 – Same as Low.<br><br>CMS-4 – Use automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior.<br><br>CMS-5 – Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.<br><br>CMS-6 – Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days. | once every seven (7) days to ensure unauthorized administrator accounts have not been created.<br><br>CMS-6 – Same as Moderate. |

| Audit and Accountability (AU) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **AU-7**<br>**Audit Reduction and Report Generation**<br>***PISP Sec. 4.3.7*** | No additional controls required beyond the referenced policy. | 1 – Employ a system capability that automatically processes audit records for events of interest based upon selectable, event criteria. | 1 – Same as Moderate. |
| **AU-8**<br>**Time Stamps**<br>***PISP Sec. 4.3.8*** | No additional controls required beyond the referenced policy. | 1 – Information system clock synchronization occurs daily and at system boot. | 1 – Same as Moderate. |
| **AU-9**<br>**Protection of Audit Information**<br>***PISP Sec. 4.3.9*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | 1 – Employ automated mechanisms that are restricted to hardware-enforced, "write-once" media for recording audit information (e.g., CD-R, not CD-RW). |
| **AU-10**<br>**Non-Repudiation**<br>***PISP Sec. 4.3.10*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **AU-11**<br>**Audit Retention**<br>***PISP Sec. 4.3.11*** | 0 – Retain audit records for ninety (90) days, and archive old audit records. Retain audit record archives for one (1) year. | 0 – Same as Low. | 0 – Same as Low. |

# 4. CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS (CA)

The standards listed in this section focus on how the organization must: (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.

**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Certification, Accreditation, and Security Assessments (CA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **CA-1**<br>**Certification, Accreditation, and Security Assessment Policy and Procedures**<br>***PISP Sec. 4.4.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **CA-2**<br>**Security Assessments**<br>***PISP Sec. 4.4.2*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **CA-3** | CMS-1 – Record each system | CMS-1 – Same as Low. | CMS-1 – Same as Low. |

| Certification, Accreditation, and Security Assessments (CA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Information System Connections**<br><br>***PISP Sec. 4.4.3*** | 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. | | |
| **CA-4**<br>**Security Certification**<br><br>***PISP Sec. 4.4.4*** | CMS-1 – Document the risk and safeguards of the system according to the CMS *Information Security Risk Assessment* (RA) *Procedures.* | 1 – Employ an independent certification agent or certification team to conduct an assessment of the information system security controls.<br><br>CMS-1 – Same as Low. | 1 – Same as Moderate.<br><br>CMS-1 – Same as Low. |
| **CA-5**<br>**Plan of Action and Milestones**<br><br>***PISP Sec. 4.4.5*** | 0 – 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. | 0 – Same as Low. | 0 – Same as Low. |
| **CA-6** | 0 – Information systems can only be accredited for a maximum | 0 – Same as Low. | 0– Same as Low. |

| Certification, Accreditation, and Security Assessments (CA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Security Accreditation**<br><br>***PISP Sec. 4.4.6*** | period of three (3) years, after which the information system must be re-accredited. | | |
| **CA-7**<br>**Continuous Monitoring**<br><br>***PISP Sec. 4.4.7*** | 1 – 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.<br><br>CMS-1 – Continuous monitoring activities include:<br>(a) Configuration management;<br>(b) Control of information system components;<br>(c) Security impact analyses of changes to the system;<br>(d) On-going assessment of security controls; and<br>(e) Status reporting. | 1 – Same as Low.<br><br>CMS-1 – Same as Low. | 1 – Same as Low.<br><br>CMS-1 – Same as Low. |

# 5. CONFIGURATION MANAGEMENT (CM)

The standards listed in this section focus on how the organization must: (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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Configuration Management (CM) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **CM-1**<br>**Configuration Management Policy and Procedures**<br>***PISP Sec. 4.5.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **CM-2**<br>**Baseline Configuration**<br>***PISP Sec. 4.5.2*** | CMS-1 – 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.<br><br>CMS-2 – Maintain an updated list of the information system's | 1 – Update the baseline configuration of the information system as an integral part of information system component installations.<br><br>CMS-1, CMS-2 – Same as Low. | 1 – Same as Moderate.<br><br>2 – Employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.<br><br>CMS-1, CMS-2 – Same as Low. |

| Configuration Management (CM) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | operations and security documentation. | | |
| **CM-3**<br>**Configuration Change Control**<br>***PISP Sec. 4.5.3*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | 1 – Employ automated mechanisms to:<br>(a) Document proposed changes to the information system,<br>(b) Notify appropriate approval authorities,<br>(c) Identify approvals that have not been received in a timely manner,<br>(d) Inhibit change until necessary approvals are received, and<br>(e) Document completed changes to the information system. |
| **CM-4**<br>**Monitoring Configuration Changes**<br>***PISP Sec. 4.5.4*** | Not required. | CMS-1 –When changes to the system occur, record the installation of information system components in the appropriate system documentation resource(s). | CMS-1 – Same as Moderate. |
| **CM-5**<br>**Access Restrictions** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | 1 – Employ automated mechanisms to enforce access restrictions and to support auditing of the enforcement |

| Configuration Management (CM) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **for Change**<br><br>***PISP Sec. 4.5.5*** | | | actions. |
| **CM-6**<br>**Configuration Settings**<br><br>***PISP Sec. 4.5.6*** | CMS-1 – 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. | CMS-1 – Same as Low. | 1 – Employ automated mechanisms to centrally manage, apply, and verify configuration settings.<br><br>CMS-1 – Same as Low. |
| **CM-7**<br>**Least Functionality**<br><br>***PISP Sec. 4.5.7*** | Not required. | 0 – 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. | 0 – Same as Moderate.<br><br>1 – 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. |
| **CM-8**<br>**Information System** | No additional controls required beyond the referenced policy. | 1 – Update the information system component inventory as an integral part of component | 1 – Same as Moderate.<br><br>2 – Employ automated |

| Configuration Management (CM) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Component Inventory**<br><br>***PISP Sec. 4.5.8*** | | installations. | mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. |

# 6. CONTINGENCY PLANNING (CP)

The standards listed in this section focus on how the organization must 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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Contingency Planning (CP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **CP-1**<br>**Contingency Planning Policy and Procedures**<br>***PISP Sec. 4.6.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **CP-2**<br>**Contingency Plan**<br>***PISP Sec. 4.6.2*** | No additional controls required beyond the referenced policy. | 1 – 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.<br><br>2 – Conduct capacity planning so | 1, 2 – Same as Moderate. |

| Contingency Planning (CP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations. | |
| **CP-3**<br>**Contingency Training**<br>***PISP Sec. 4.6.3*** | 0 – Provide training every 365 days in contingency roles and responsibilities. | 0 – Same as Low. | 0 – Same as Low.<br><br>1 – Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.<br><br>2 – Employ automated mechanisms to provide thorough and realistic training environments. |
| **CP-4**<br>**Contingency Plan Testing and Exercises**<br>***PISP Sec. 4.6.4*** | 0 – The CP must be current and executable, tested using a combination of tabletop exercises and operational tests every 365 days, and updated as needed. | 0 – Same as Low.<br><br>1 – Coordinate testing and exercising of CP with parties responsible for related plans, such as:<br>(a) Business Continuity Plan,<br>(b) Disaster Recovery Plan,<br>(c) Continuity of Operations Plan,<br>(d) Business Recovery Plan, and<br>(e) Incident Response Plan. | 0 – Same as Low.<br><br>1 – Same as Moderate.<br><br>2 – Test / exercise the CP at the alternate processing site to evaluate the site's capabilities to support contingency operations.<br><br>3 – Employ automated mechanisms to more thoroughly |

| Contingency Planning (CP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | | 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. |
| **CP-5**<br>**Contingency Plan Update**<br>***PISP Sec. 4.6.5*** | 0 – 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. | 0 – Same as Low. | 0 – Same as Low. |
| **CP-6**<br>**Alternate Storage Site**<br>***PISP Sec. 4.6.6*** | Not required. | 1 – Ensure that the alternate storage site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.<br><br>2 – Not required.<br><br>3 – Identify potential accessibility | 1 – Same as Moderate.<br><br>2 – Ensure that the alternate storage site is configured to facilitate timely and effective recovery operations.<br><br>3 – Same as Moderate. |

| Contingency Planning (CP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | problems to the alternate storage site in the event of an area-wide disruption or disaster and document explicit mitigation actions. | |
| **CP-7**<br>**Alternate Processing Site**<br>***PISP Sec. 4.6.7*** | Not required. | 0 – 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.<br><br>1 – Ensure the alternate processing site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.<br><br>2 – Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. | 0 – 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.<br><br>1 thru 3 – Same as Moderate.<br><br>4 – Ensure the alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site. |

| Contingency Planning (CP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | 3 – Ensure alternate processing site agreements contain appropriate priority-of-service provisions. | |
| **CP-8**<br>**Telecommunications Services**<br>***PISP Sec. 4.6.8*** | Not required. | 0 – Resume system operations for critical functions within seventy-two (72) hours when the primary telecommunications capabilities are unavailable.<br><br>1 – Ensure agreements with primary and alternate telecommunication service providers include priority-of-service provisions.<br><br>2 – Ensure alternate telecommunication providers do not share a single point of failure with primary telecommunications services. | 0 – Resume system operations for critical functions within twelve (12) hours when the primary telecommunications capabilities are unavailable.<br><br>1, 2 – Same as Moderate.<br><br>3 – Ensure alternate telecommunications service providers are sufficiently separated from the primary telecommunications services, to prevent susceptibility to the same hazards.<br><br>4 – Ensure that primary and alternate telecommunication service providers have adequate CPs. |
| **CP-9** | 0 – Perform backups of user-level and system-level | 0 – Perform full backups weekly to separate media. Perform | 0 – Perform full backups to separate media every other day. |

| Contingency Planning (CP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Information System Backup**<br><br>***PISP Sec. 4.6.9*** | information (including system state information) every month. | 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.<br><br>1 – Test backup information to verify media reliability and information integrity, following each backup.<br><br>2, 3 – Not required.<br><br>4 – Protect backup information from unauthorized modification. | 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.<br><br>1 – Same as Moderate.<br><br>2 – Use select backup information to restore information systems as part of the Contingency Plan testing.<br><br>3 – 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 |

| Contingency Planning (CP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | | operational software.<br><br>4 – Same as Moderate. |
| **CP-10**<br><br>**Information System Recovery and Reconstitution**<br><br>***PISP Sec. 4.6.10*** | 0 – Secure information system recovery and reconstitution includes, but not limited to:<br>(a) Reset all system parameters (either default or organization-established),<br>(b) Reinstall patches,<br>(c) Reestablish configuration settings,<br>(d) Reinstall application and system software, and<br>(e) Fully test the system. | 0 – Same as Low. | 0 – Same as Low.<br><br>1 – Perform full recovery and reconstitution of the information system as part of CP testing. |

# 7. IDENTIFICATION AND AUTHENTICATION (IA)

The standards listed in this section focus on how the organization must 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.

**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Identification and Authentication (IA) Standard | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **IA-1**<br>**Identification and Authentication Policy and Procedures**<br>***PISP Sec. 4.7.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **IA-2**<br>**User Identification and Authentication**<br>***PISP Sec. 4.7.2*** | CMS-1 – Require the use of unique user identifiers and system and/or network authenticators.<br><br>CMS-2 – All passwords shall be encrypted in transit and at rest.<br><br>CMS-3 – Help desk support requires user identification for any | 1 – Employ multifactor authentication for remote system access that is at least NIST SP 800-63 level 3 compliant.<br><br>CMS-1 thru CMS-3 – Same as Low. | 1 – Not applicable.<br><br>2 – Employ multifactor authentication for local system access that is at least NIST SP 800-63 level 3 compliant.<br><br>3 – Employ multifactor authentication for remote system |

| Identification and Authentication (IA) Standard | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | transaction that has information security implications. | | access that is NIST SP 800-63 level 4 compliant.<br><br>CMS-1 thru CMS-3 – Same as Low. |
| **IA-3**<br>**Device Identification and Authentication**<br><br>***PISP Sec. 4.7.3*** | 0 – Implement an information system that uses either a shared secret or digital certificate to identify and authenticate specific devices before establishing a connection. | 0 – Same as Low. | 0 – Same as Low. |
| **IA-4**<br>**Identifier Management**<br><br>***PISP Sec. 4.7.4*** | 0 – Disable user identifiers after 365 days of inactivity and delete disabled accounts during annual re-certification process.<br><br>CMS-1 – 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.<br><br>CMS-2 –For non-CMS entities to issue user identifiers, receive prior | 0 – Same as Low except after 180 days of inactivity.<br><br>CMS-1, CMS-2 – Same as Low. | 0 – Same as Low except after 90 days of inactivity.<br><br>CMS-1, CMS-2 – Same as Low. |

| Identification and Authentication (IA) Standard | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | written approval from the CIO or his/her designated representative. | | |
| **IA-5**<br>**Authenticator Management**<br>***PISP Sec. 4.7.5*** | 0 – For password-based authentication:<br>(a) Protect passwords from disclosure or modification when stored or transmitted,<br>(b) Prevent passwords from being displayed when entered,<br>(c) When using passwords in connection with e-authentication, refer to ARS Appendix A, *e-Authentication Standards* for further guidance,<br>(d) Force users to select a password comprising a minimum of eight (8) alphanumeric and/or special characters,<br>(e) Automatically force users (including administrators) to change account and system account passwords after sixty (60) days,<br>(f) Automatically force users to | 0 – Same as Low except:<br>(f) Automatically force users to select six (6) unique passwords prior to reusing a previous one. | 0 – Same as Moderate except:<br>(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. |

| Identification and Authentication (IA) Standard | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | select one (1) unique password prior to reusing a previous one, and<br>(g) Enforce password lifetime restrictions within a minimum of one (1) day and maximum of sixty (60) days. | | |
| **IA-6**<br>**Authenticator Feedback**<br>***PISP Sec. 4.7.6*** | 0 – Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). | 0 – Same as Low. | 0 – Same as Low. |
| **IA-7**<br>**Cryptographic Module Authentication**<br>***PISP Sec. 4.7.7*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

## 8. INCIDENT RESPONSE (IR)

The standards listed in this section focus on how the organization must: (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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Incident Response (IR) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **IR-1**<br>**Incident Response Policy and Procedures**<br>***PISP Sec. 4.8.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **IR-2**<br>**Incident Response Training**<br>***PISP Sec. 4.8.2*** | Not required. | 0 – Provide training on incident response roles and responsibilities of personnel every 365 days. | 0 – Same as Moderate.<br><br>1 – Incorporate simulated events as part of incident response training.<br><br>2 – Employ automated mechanisms to provide a more thorough and realistic incident response training environment. |
| **IR-3** | Not required. | 0 – Test and/or exercise and | 0 – Same as Moderate. |

| Incident Response (IR) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Incident Response Testing and Exercises**<br><br>***PISP Sec. 4.8.3*** | | document the incident response capability every 365 days, using reviews, analyses, and simulations. | 1 – Employ automated mechanisms to test / exercise the incident response plan. |
| **IR-4**<br>**Incident Handling**<br><br>***PISP Sec. 4.8.4*** | CMS-1 – Document relevant information related to a security incident according to CMS *Information Security Incident Handling and Breach Notification Procedures*.<br><br>CMS-2 – 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.<br><br>CMS-3 – Identify vulnerability exploited during a security incident. Implement security | 1 – Employ automated mechanisms to support the incident handling process.<br><br>CMS-1 thru CMS-3 – Same as Low. | 1 – Same as Moderate.<br><br>CMS-1, CMS-2 – Same as Low.<br><br>CMS-3 – Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure, including isolation or system disconnect. |

| Incident Response (IR) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | safeguards to reduce risk and vulnerability exploit exposure. | | |
| **IR-5**<br>**Incident Monitoring**<br>***PISP Sec. 4.8.5*** | Not required. | No additional controls required beyond the referenced policy. | 1 – Employ automated mechanisms to assist in tracking and analyzing security incidents |
| **IR-6**<br>**Incident Reporting**<br>***PISP Sec. 4.8.6*** | No additional controls required beyond the referenced policy. | 1 – Employ automated mechanisms to assist in the reporting of security incidents. | 1 – Same as Moderate. |
| **IR-7**<br>**Incident Response Assistance**<br>***PISP Sec. 4.8.7*** | No additional controls required beyond the referenced policy. | 1 – Employ automated mechanisms to increase the availability of incident response-related information and support. | 1 – Same as Moderate. |

# 9. MAINTENANCE (MA)

The standards listed in this section focus on how the organization must: (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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Maintenance (MA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **MA-1**<br>**System Maintenance Policy and Procedures**<br>***PISP Sec. 4.9.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **MA-2**<br>**Controlled Maintenance**<br>***PISP Sec. 4.9.2*** | No additional controls required beyond the referenced policy. | 1 – Maintain maintenance records for each information system that includes:<br>(a) Date and time of maintenance,<br>(b) Name of the individual performing the maintenance, name of escort, if applicable,<br>(c) Description of the maintenance performed, and<br>(d) List of equipment removed or replaced (including | 1 – Same as Moderate.<br><br>2 – 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. |

| Maintenance (MA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | identification numbers, if applicable). | |
| **MA-3**<br>**Maintenance Tools**<br>***PISP Sec. 4.9.3*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | 1 – Inspect all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.<br><br>2 – Check all media containing diagnostic and test programs for malicious code before the media is used in the system.<br><br>3 – 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. |

| Maintenance (MA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | | 4 – Employ automated mechanisms to restrict the use of maintenance tools to authorized personnel only. |
| **MA-4**<br>**Remote Maintenance**<br>***PISP Sec. 4.9.4*** | CMS-1 – If remote maintenance is authorized in writing by the CIO or his/her designated representative:<br>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. | 1 – Audit all remote maintenance sessions, and ensure that appropriate information security personnel review the maintenance records of the remote sessions.<br><br>2 – Document the use of remote diagnostic tools in the SSP.<br><br>CMS-1 – Same as Low. | 1, 2 – Same as Moderate.<br><br>3 – 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 |

| Maintenance (MA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | | failure), remote maintenance is not permitted.<br><br>CMS-1 – Same as Low. |
| **MA-5**<br>**Maintenance Personnel**<br>***PISP Sec. 4.9.5*** | 0 – 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. | 0 – Same as Low. | 0 – Same as Low. |
| **MA-6**<br>**Timely Maintenance**<br>***PISP Sec. 4.9.6*** | Not required. | 0 – 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. | 0 – Same as Moderate. |
| **MA-CMS-1** | CMS-0 – Access to system for | CMS-0 – Same as Low. | CMS-0 – Same as Low. |

| Maintenance (MA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Off-site Physical Repair of Systems**<br><br>***PISP Sec. 4.9.7*** | 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. | | |
| **MA-CMS-2**<br>**On-site Physical Repair of Systems**<br><br>***PISP Sec. 4.9.8*** | CMS-1 – Access to system for repair must be by authorized personnel only. | CMS-1– Same as Low.<br><br>CMS-2 – Physical repair of servers must be within protected environments. | CMS-1 – Same as Low.<br><br>CMS-2 – Same as Moderate. |

## 10. MEDIA PROTECTION (MP)

The standards listed in this section focus on how the organization must: (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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Media Protection (MP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **MP-1**<br>**Media Protection Policy and Procedures**<br>***PISP Sec. 4.10.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **MP-2**<br>**Media Access**<br>***PISP Sec. 4.10.2*** | No additional controls required beyond the referenced policy. | 1 – Employ automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. | 1 – Same as Moderate. |
| **MP-3**<br>**Media Labeling**<br>***PISP Sec. 4.10.3*** | Not required. | CMS-1 – Off-line backup storage media must be marked according to backup rotation schedule for ease of retrieval. | CMS-1 – Same as Moderate. |
| **MP-4** | No additional controls required | No additional controls required | No additional controls required |

| Media Protection (MP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Media Storage**<br><br>***PISP Sec. 4.10.4*** | beyond the referenced policy. | beyond the referenced policy. | beyond the referenced policy. |
| **MP-5**<br>**Media Transport**<br><br>***PISP Sec. 4.10.5*** | Not required. | 1 – 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.<br>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 | 1, 2 – Same as Moderate.<br><br>3 – Employ an identified custodian at all times to transport information system media. |

| Media Protection (MP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | with return receipt in tamper-proof packaging.<br>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).<br><br>2 – Activities associated with the transport of sensitive information system media are documented. | |
| **MP-6**<br>**Media Sanitization and Disposal**<br><br>***PISP Sec. 4.10.6*** | No additional controls required beyond the referenced policy. | 0 – The sanitization process includes the removal of all data, labels, marking, and activity records using NSA Guidance (http://www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, *Guidelines for Media Sanitization.*<br>*CMS-1* – Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, | 0 – Same as Moderate.<br><br>CMS-1 – Same as Moderate. |

| Media Protection (MP) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | and procedures. | |
| **MP-CMS-1**<br>**Media Related Records**<br>***PISP Sec. 4.10.7*** | Not required. | CMS-0 –The media records must, at a minimum, contain:<br>(a) the name of media recipient;<br>(b) signature of media recipient;<br>(c) date / time media received;<br>(d) media control number and contents;<br>(e) movement or routing information; and<br>(f) if disposed of, the date, time, and method of destruction. | CMS-0 – Same as Moderate. |

# 11. PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

The standards listed in this section focus on how the organization must: (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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Physical and Environmental Protection (PE) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **PE-1**<br>**Physical and Environmental Protection Policy and Procedures**<br>***PISP Sec. 4.11.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PE-2**<br>**Physical Access Authorizations**<br>***PISP Sec. 4.11.2*** | 0 – Review and approve lists of personnel with authorized access to facilities containing information systems at least once every 365 days. | 0 – Review and approve lists of personnel with authorized access to facilities containing information systems at least once every 180 days. | 0 – Review and approve lists of personnel with authorized access to facilities containing information systems at least once every 90 days.. |

| Physical and Environmental Protection (PE) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **PE-3**<br>**Physical Access Control**<br>***PISP Sec. 4.11.3*** | CMS-1 – Control data center / facility access by use of door and window locks.<br><br>CMS-2 – Store and operate servers in physically secure environments protected from unauthorized access.<br><br>CMS-3 – Data centers must meet the minimum requirements as established by the *Federal Information Systems Control Audit Manual (FISCAM).* | CMS-1 – 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.<br><br>CMS-2 – Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.<br><br>CMS-3 – Same as Low.<br><br>CMS-4 – Restrict access to grounds / facilities to authorized persons only. | 1 – Physical access control to the information system is independent of the physical access controls for the facility.<br><br>CMS-1, CMS-2, CMS-4 – Same as Moderate.<br><br>CMS-3 – Same as Low. |
| **PE-4**<br>**Access Control for Transmission Media**<br>***PISP Sec. 4.11.4*** | CMS-1 – Prohibit public access to telephone closets and information system distribution and transmission lines within organizational facilities. | CMS-1 – Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel. | CMS-1 – Same as Moderate.<br><br>CMS-2 – Same as Low. |

| Physical and Environmental Protection (PE) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | CMS-2 – Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use. | CMS-2 – Same as Low. | |
| **PE-5**<br>**Access Control for Display Medium**<br>***PISP Sec. 4.11.5*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PE-6**<br>**Monitoring Physical Access**<br>***PISP Sec. 4.11.6*** | No additional controls required beyond the referenced policy. | 1 – Monitor real-time physical intrusion alarms and surveillance equipment. | 1– Same as Moderate.<br><br>2 – Automated mechanisms are implemented to recognize potential intrusions and initiate appropriate response actions. |
| **PE-7**<br>**Visitor Control**<br>***PISP Sec. 4.11.7*** | No additional controls required beyond the referenced policy. | 1 – Escort visitors and monitor visitor activity. | 1 – Same as Moderate. |
| **PE-8**<br>**Access Records**<br>***PISP Sec. 4.11.8*** | 0 – Visitor access records must be closed out and reviewed by management monthly. | 0 – Same as Low. | 0 – Same as Low.<br><br>1 – Employ automated mechanisms to facilitate the maintenance and review of |

| Physical and Environmental Protection (PE) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | | access records.<br><br>2 – Maintain records of all physical access, both visitor and authorized individuals. |
| **PE-9**<br>**Power Equipment and Cabling**<br>***PISP Sec. 4.11.9*** | CMS-1 – Prohibit public access to infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.<br><br>CMS-2 – Power surge protection must be implemented for all computer equipment. | CMS-1 – Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.<br><br>CMS-2 – Same as Low. | 1 – Employ redundant and parallel power cabling paths.<br><br>CMS-1 – Same as Moderate.<br><br>CMS-2 – Same as Low. |
| **PE-10**<br>**Emergency Shutoff**<br>***PISP Sec. 4.11.10*** | Not required. | CMS-1 – 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. | 1 – Employ appropriate measures to protect the emergency power-off capability from accidental and intentional / unauthorized activation.<br><br>CMS-1 – Same as Moderate. |
| **PE-11**<br>**Emergency Power**<br>***PISP Sec. 4.11.11*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | 1 – Provide a long-term alternate power supply for the system that is capable of maintaining minimally required operational |

| Physical and Environmental Protection (PE) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | | capability in the event of an extended loss of the primary power source. |
| **PE-12**<br>**Emergency Lighting**<br>***PISP Sec. 4.11.12*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PE-13**<br>**Fire Protection**<br>***PISP Sec. 4.11.13*** | No additional controls required beyond the referenced policy. | 1 – Implement and maintain fire detection devices / systems that activate automatically and notify the organization and emergency responders in the event of a fire.<br><br>2 – Employ fire suppression devices / systems that provide automatic notification of any activation to the organization and emergency responders.<br><br>3 – Employ an automatic fire suppression capability in facilities that are not staffed on a continuous basis. | 1 thru 3 – Same as Moderate. |
| **PE-14** | CMS-1 – Evaluate the level of | CMS-1 – Same as Low. | CMS-1 – Same as Low. |

| Physical and Environmental Protection (PE) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Temperature and Humidity Controls**<br><br>***PISP Sec. 4.11.14*** | alert and follow prescribed guidelines for that alert level. | CMS-2 – Alert component management of possible loss of service and/or media.<br><br>CMS-3 – Report damage and provide remedial action. Implement contingency plan, if necessary. | CMS-2, CMS-3 – Same as Moderate. |
| **PE-15**<br>**Water Damage Protection**<br><br>***PISP Sec. 4.11.15*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | 1 – 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. |
| **PE-16**<br>**Delivery and Removal**<br><br>***PISP Sec. 4.11.16*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PE-17** | No additional controls required beyond the referenced policy. | CMS-1 – Employ appropriate security controls at alternate work | CMS-1 – Same as Moderate. |

| Physical and Environmental Protection (PE) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Alternate Work Site**<br><br>***PISP Sec. 4.11.17*** | | 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. | |
| **PE-18**<br>**Location of Information System Components**<br><br>***PISP Sec. 4.11.18*** | Not required. | No additional controls required beyond the referenced policy. | 1 – 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. |
| **PE-19**<br>**Information Leakage**<br><br>***PISP Sec. 4.11.19*** | Not required. | Not required. | Not required. |

## 12. PLANNING (PL)

The standards listed in this section focus on how the organization must 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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Planning (PL) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **PL-1**<br>**Security Planning Policy and Procedures**<br>***PISP Sec. 4.12.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PL-2**<br>**System Security Plan**<br>***PISP Sec. 4.12.2*** | CMS-1 – Document the in-place security controls of the system according to the *CMS System Security Plan (SSP) Procedures*. | CMS-1 – Same as Low. | CMS-1 – Same as Low. |
| **PL-3**<br>**System Security Plan Update**<br>***PISP Sec. 4.12.3*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

| Planning (PL) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **PL-4**<br>**Rules of Behavior**<br>***PISP Sec. 4.12.4*** | CMS-1 – Define user roles and expectations for system and network use.<br><br>CMS-2 – Electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). | CMS-1, CMS-2 – Same as Low. | CMS-1, CMS-2 – Same as Low. |
| **PL-5**<br>**Privacy Impact Assessment**<br>***PISP Sec. 4.12.5*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PL-6**<br>**Security-Related Activity Planning**<br>***PISP Sec. 4.12.6*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

## 13. PERSONNEL SECURITY (PS)

The standards listed in this section focus on how the organization must: (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.

**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Personnel Security (PS) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **PS-1**<br>**Personnel Security Policy and Procedures**<br>***PISP Sec. 4.13.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PS-2**<br>**Position Categorization**<br>***PISP Sec. 4.13.2*** | 0 – Review and revise position risk designations every 365 days. | 0 – Same as Low. | 0 – Same as Low. |
| **PS-3** | 0 – Perform criminal history check | 0 – Same as Low. | 0 – Same as Low. |

| Personnel Security (PS) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Personnel Screening**<br><br>***PISP Sec. 4.13.3*** | for all persons prior to employment.<br><br>CMS-1 – Require personnel to obtain and hold a low-risk security clearance as defined in *DHHS Personnel Security/Suitability Handbook*. | CMS-1 – Require personnel to obtain and hold a moderate-risk security clearance as defined in the *DHHS Personnel Security/Suitability Handbook.* | CMS-1 – Require personnel to obtain and hold a high-risk security clearance as defined in the *DHHS Personnel Security/Suitability Handbook*. |
| **PS-4**<br>**Personnel Termination**<br><br>***PISP Sec. 4.13.4*** | CMS-1 – Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination.. | CMS-1 – Same as Low except immediately following employee termination, and system access must be revoked prior to or during the employee termination process. | CMS-1 – Same as Moderate. |
| **PS-5**<br>**Personnel Transfer**<br><br>***PISP Sec. 4.13.5*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PS-6**<br>**Access Agreements**<br><br>***PISP Sec. 4.13.6*** | 0 – Access agreements are reviewed and updated as part of the system accreditation or when a contract is renewed or extended. | 0 – Same as Low. | 0 – Same as Low. |
| **PS-7**<br>**Third Party Personnel Security** | CMS-1 – Regulate the access provided to contractors and define security requirements for contractors. Contractors must be | CMS-1 – Same as Low. | CMS-1 – Same as Low. |

| Personnel Security (PS) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| ***PISP Sec. 4.13.7*** | 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**<br>**Personnel Sanctions**<br><br>***PISP Sec. 4.13.8*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PS-CMS-1**<br>**Review System Access during Extraordinary Personnel Circumstances**<br><br>PISP Sec. 4.13.9 | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **PS-CMS-2**<br>**Designate an** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

| Personnel Security (PS) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Information System Security Officer (ISSO) / System Security Officer (SSO)**<br><br>***PISP Sec. 4.13.10*** | | | |

## 14. RISK ASSESSMENT (RA)

The standards listed in this section focus on how the organization must 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.
**NOTE:** When a control for a system is subject to higher standards to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| Risk Assessment (RA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **RA-1**<br>**Risk Assessments Policy and Procedures**<br>***PISP Sec. 4.14.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **RA-2**<br>**Security Categorization**<br>***PISP Sec. 4.14.2*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **RA-3** | CMS-1 – Perform an IS RA for | CMS-1 – Same as Low. | CMS-1 – Same as Low. |

| Risk Assessment (RA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Risk Assessments (RA)**<br><br>***PISP Sec. 4.14.3*** | 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]*). | | |
| **RA-4**<br>**Risk Assessment Update**<br><br>***PISP Sec. 4.14.4*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **RA-5**<br>**Vulnerability Scanning**<br><br>***PISP Sec. 4.14.5*** | CMS-1 – 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. | 0 – 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.<br><br>CMS-1 – Same as Low. | 0 – Same as Moderate.<br><br>1 – Vulnerability scanning tools must include the capability to readily update the list of vulnerabilities scanned.<br><br>2 – Update the list of system vulnerabilities scanned every 365 days or when significant new vulnerabilities are identified and reported.<br><br>3 – Perform internal network |

| Risk Assessment (RA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | | 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.<br><br>CMS–1 – Same as Low. |

## 15. SYSTEM AND SERVICES ACQUISITION (SA)

The standards listed in this section focus on how the organization must: (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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| System and Services Acquisition (SA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SA-1**<br>**System and Services Acquisition Policy and Procedures**<br>***PISP Sec. 4.15.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SA-2**<br>**Allocation of Resources**<br>***PISP Sec. 4.15.2*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

| System and Services Acquisition (SA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SA-3**<br>**Life Cycle Support**<br>***PISP Sec. 4.15.3*** | CMS-1 – Must comply with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK. | CMS-1 – Same as Low. | CMS-1 – Same as Low. |
| **SA-4**<br>**Acquisitions**<br>***PISP Sec. 4.15.4*** | CMS-1 – 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. | 1 – 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.<br><br>CMS-1 – Same as Low. | 1 – Same as Moderate.<br><br>CMS-1 – Same as Low. |
| **SA-5**<br>**Information System Documentation**<br>***PISP Sec. 4.15.5*** | CMS-1 – Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.<br><br>CMS-2 – Maintain an updated list of related system operations and | 1 – 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. | 1 – Same as Moderate.<br><br>2 – Ensure that system documentation describes the design and implementation details of the security controls implemented within the information system with sufficient detail to permit |

| System and Services Acquisition (SA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | security documentation.<br><br>CMS-3 – 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. | CMS-1 thru CMS-3 – Same as Low.<br><br>CMS-4 – Document the system's configuration, and procedures in support of system access administration and operations. | analysis and testing of the controls.<br><br>CMS-1 thru CMS-3 – Same as Low.<br><br>CMS-4 – Same as Moderate. |
| **SA-6**<br>**Software Usage Restrictions**<br><br>***PISP Sec. 4.15.6*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SA-7**<br>**User Installed Software**<br><br>***PISP Sec. 4.15.7*** | CMS-1 – 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. | CMS-1 – Same as Low. | CMS-1 – Same as Low. |

| System and Services Acquisition (SA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SA-8**<br>**Security Engineering Principles**<br>***PISP Sec. 4.15.8*** | Not required. | 0 – 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).* | 0 – Same as Moderate. |
| **SA-9**<br>**External Information System Services**<br>***PISP Sec. 4.15.9*** | CMS-1 – 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. | CMS-1 – Same as Low. | CMS-1 – Same as Low. |

| System and Services Acquisition (SA) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SA-10**<br>**Developer Configuration Management**<br>***PISP Sec. 4.15.10*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SA-11**<br>**Developer Security Testing**<br>***PISP Sec. 4.15.11*** | Not required. | CMS-1 – 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.<br><br>CMS-2 – Use hypothetical data when executing test scripts. | CMS-1, CMS-2– Same as Moderate. |

## 16. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

The standards listed in this section focus on how the organization must: (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.
**NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SC-1**<br>**System and Communications Protection Policy and Procedures**<br>***PISP Sec. 4.16.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SC-2**<br>**Application Partitioning**<br>***PISP Sec. 4.16.2*** | CMS-1 – Implement DMZ architecture to separate internal network from public systems, and CMS servers from unnecessary public access, physically partitioning applications of varying sensitivity levels. | CMS-1 – 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 | CMS-1 – Same as Moderate. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | proxy rules to provide protection for CMS servers. | |
| **SC-3**<br>**Security Function Isolation**<br>***PISP Sec. 4.16.3*** | Not required. | No additional controls required beyond the referenced policy. | 1 – Employ hardware separation mechanisms to facilitate the isolation of security functions.<br><br>2 – Isolate critical security functions from both non-security functions and other security functions.<br><br>3 – Minimize the number of non-security functions included within the isolation boundary containing security functions.<br><br>4 – Implement security functions in largely independent modules that avoid unnecessary interactions between modules.<br><br>5 – Implement security functions in a layered structure minimizing interactions between layers of the design and avoiding any |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | | dependence by lower layers on the functionality or correctness of higher layers. |
| **SC-4**<br>**Information Remnance**<br>***PISP Sec. 4.16.4*** | Not required. | 0 – 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. | 0 – Same as Moderate. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SC-5**<br>**Denial-of-Service Protection**<br>***PISP Sec. 4.16.5*** | 0 – Protect the information system against the denial-of-service attacks defined on the following sites or within the following documents:<br>• SANS Organization http://www.sans.org/dosstep;<br>• SANS Organization's Roadmap to Defeating DDoS http://www.sans.org/dosstep/roadmap.php; and<br>• NIST CVE List http://checklists.nist.gov/home.cfm .<br><br>1 – Restrict the ability of users to launch denial of service attacks against other information systems or networks.<br><br>2 – Maintain excess capacity, bandwidth, or other redundancy to limit the effects of information | 0 thru 2 – Same as Low. | 0 thru 2 – Same as Low. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | flooding types of denial of service attacks. | | |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SC-6**<br>**Resource Priority**<br>***PISP Sec. 4.16.6*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SC-7**<br>**Boundary Protection**<br>***PISP Sec. 4.16.7*** | 1 thru 4 – Not required.<br><br>5 – Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.<br><br>CMS-1 – Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.<br><br>CMS-2 – Although not required, it is recommended that stateful inspection hardware and software is utilized. | 1 – 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.<br><br>2 – Prevent public access into the internal networks except as appropriately mediated.<br><br>3 – Limit the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.<br><br>4 – Maintain a managed interface with any external | 1 thru 4 – Same as Moderate.<br><br>5 – Same as Low.<br><br>CMS-1 – Same as Low.<br><br>CMS-2, CMS-3 – Same as Moderate. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.<br><br>5, CMS-1 – Same as Low.<br><br>CMS-2 – Utilize stateful inspection / application firewall hardware and software.<br><br>CMS-3 – 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. | |
| **SC-8**<br>**Transmission Integrity**<br><br>***PISP Sec. 4.16.8*** | Not required. | 1 – Employ approved cryptographic mechanisms to ensure recognition of changes to information during transmission.<br><br>CMS-1 – Employ appropriate | 1, CMS-1 – Same as Moderate. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | 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**<br>**Transmission Confidentiality**<br>***PISP Sec. 4.16.9*** | Not required. | 1 – Encryption is not required within a secured network. When transmitting data outside of a secured network:<br>(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<br>(b) Either a VPN or dedicated leased lines/circuits must be used. | 1 – Same as Moderate. |
| **SC-10**<br>**Network Disconnect**<br>***PISP Sec. 4.16.10*** | 0 – Configure the information system to forcibly disconnect network connections at the end of a session, or after fifteen (15) minutes of inactivity, for | 0 – Same as Low. | 0 – Same as Low. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | mainframe sessions. | | |
| **SC-11**<br>**Trusted Path**<br>***PISP Sec. 4.16.11*** | Not required. | 0 – 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. | 0 – Same as Moderate. |
| **SC-12**<br>**Cryptographic Key Establishment and Management**<br>***PISP Sec. 4.16.12*** | Not required. | CMS-1 – 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 | CMS-1 – Same as Moderate. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | | key owner, and comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13). | |
| **SC-13**<br>**Use of Cryptography**<br>***PISP Sec. 4.16.13*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SC-14**<br>**Public Access Protections**<br>***PISP Sec. 4.16.14*** | CMS-1 – 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.<br><br>CMS-2 – 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. | CMS-1-CMS-2 – Same as Low. | CMS-1-CMS-2 – Same as Low. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SC-15**<br>**Collaborative Computing**<br>***PISP Sec. 4.16.15*** | Not required. | If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:<br><br>1 – Provide physical disconnect of cameras or microphones in a manner that supports ease of use.<br><br>CMS-1 – Ensure the information system provides:<br>An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and<br>Explicit indication to the local user of the fact that it is in use. | If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:<br><br>1, CMS-1 – Same as Moderate. |
| **SC-16**<br>**Transmission of Security Parameters** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| ***PISP Sec. 4.16.16*** | | | |
| **SC-17**<br>**Public Key Infrastructure Certificates**<br>***PISP Sec. 4.16.17*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SC-18**<br>**Mobile Code**<br>***PISP Sec. 4.16.18*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SC-19**<br>**Voice Over Internet Protocol**<br>***PISP Sec. 4.16.19*** | Not required. | CMS-1 – The use of VoIP must be authorized in writing by the CMS CIO, or his/her designated representative. | CMS-1 – Same as Moderate. |
| **SC-20**<br>**Secure Name /Address Resolution Service (Authoritative** | Not required. | No additional controls required beyond the referenced policy. | 1 – When the information system is operating as part of a distributed, hierarchical namespace, ensure that it provides the means to indicate |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Source)**<br><br>***PISP Sec. 4.16.20*** | | | 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. |
| **SC-21**<br>**Secure Name /Address Resolution Service (Recursive or Caching Resolver)**<br><br>***PISP Sec. 4.16.21*** | Not required. | Not required. | No additional controls required beyond the referenced policy. |
| **SC-22**<br>**Architecture and Provisioning for Name /Address Resolution Service** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| ***PISP Sec. 4.16.22*** | | | |
| **SC-23**<br>**Session Authenticity**<br>***PISP Sec. 4.16.23*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SC-CMS-1**<br>**Desktop Modems**<br>***PISP Sec. 4.16.24*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SC-CMS-2**<br>**Identify and Detect Unauthorized Modems**<br>***PISP Sec. 4.16.25*** | CMS-0 – Examine a sample of network systems using an automated method no less than quarterly to determine if unauthorized modems are present. | CMS-0 – 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. | CMS-0 – Same as Moderate. |
| **SC-CMS-3**<br>**Secondary Authentication and Encryption**<br>***PISP Sec. 4.16.26*** | CMS-0 – No specific requirements but recommend enabling application security mechanisms, such as Transport Layer Security (TLS), and utilizing minimum encryption and password authentication. | CMS-0 – Enable application security mechanisms, such as Transport Layer Security (TLS). Utilize CMS-approved encryption and password authentication methods. | CMS-0 – 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- |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | CMS-1 – If e-authentication is required and implemented, refer to ARS Appendix A for *e-Authentication Standards* controls and procedures. | CMS-1 – Same as Low. | based authentication or additional authentication protection (e.g., token-based, biometric).<br><br>CMS-1 – Same as Low. |
| **SC-CMS-4**<br>**Electronic Mail**<br><br>***PISP Sec. 4.16.27*** | Not required. | CMS-0 – Prior to sending an email, place all CMS sensitive information in an encrypted attachment. | CMS-0 – Same as Moderate. |
| **SC-CMS-5**<br>**Persistent Cookies**<br><br>***PISP Sec. 4.16.28*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SC-CMS-6**<br>**Network Interconnection**<br><br>***PISP Sec. 4.16.29*** | CMS-0 – 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 | CMS-0 – Same as Low. | CMS-0 – Same as Low. |

| System and Communications Protection (SC) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | interconnection in the SSP for the system that is connected to the remote location. | | |

## 17. SYSTEM AND INFORMATION INTEGRITY (SI)

The standards listed in this section focus on how the organization must: (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. **NOTE:** When a control for a system is subject to higher standards in order to meet specific federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

| System and Information Integrity (SI) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **SI-1**<br>**System and Information Integrity Policy and Procedures**<br>***PISP Sec. 4.17.1*** | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SI-2**<br>**Flaw Remediation**<br>***PISP Sec. 4.17.2*** | 0 – Correct identified information system flaws on production equipment within one (1) month.<br>(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential | 0 – Same as Low except implement within one (1) week.<br>1-2 – Same as Low. | 0 – Same as Low except implement within seventy-two (72) hours.<br>1-2 – Same as Low. |

| System and Information Integrity (SI) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | side effects of such changes, and<br>(b) Manage the flaw remediation process centrally.<br><br>1 –Updates are installed automatically.<br><br>2 – Employ automated mechanisms periodically and upon demand to determine the state of information system components with regard to flaw remediation. | | |
| **SI-3**<br>**Malicious Code Protection**<br><br>***PISP Sec. 4.17.3*** | 0 – 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. | 0 thru 2 – Same as Low.<br><br>CMS-1 – Same as Low except every twenty-four (24) hours. | 0 thru 2 – Same as Low.<br><br>CMS-1 –Same as Low except every twelve (12) hours. |

| System and Information Integrity (SI) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| | 1 – Manage and update malicious code protection software centrally with automatic updates for the latest malicious code definitions whenever new releases are available.<br><br>2 – Employ automated mechanisms to update malicious code protection.<br><br>CMS-1 – 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. | | |
| **SI-4**<br>**Information System Monitoring Tools** | 1 – Connect individual IDS devices to a common IDS management network using | 1 – Same as Low.<br><br>2, 3 – Not required. | 1 – Same as Low.<br><br>2 – Employ automated |

| System and Information Integrity (SI) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **and Techniques**<br><br>***PISP Sec. 4.17.4*** | common protocols.<br><br>2 thru 4 – Not required.<br><br>5 – Real-time alerts are provided when indications of the following types of compromise, or potential compromise, occur:<br>(a) Presence of malicious code,<br>(b) Unauthorized export of information,<br>(c) Signaling to an external information system, or<br>(d) Potential intrusions.<br><br>CMS-1 – Install IDS devices at network perimeter points and host-based IDS sensors on critical servers. | 4 – Monitor inbound and outbound communications for unusual or unauthorized activities or conditions.<br><br>5, CMS-1 – Same as Low. | information system monitoring tools to support near-real-time analysis of events.<br><br>3 – 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.<br><br>4 – Same as Moderate.<br><br>5, CMS-1 – Same as Low. |
| **SI-5**<br>**Security Alerts and Advisories** | No additional controls required beyond the referenced policy. | 1 – Employ automated mechanisms to make security alerts and advisory information available to all appropriate | 1– Same as Moderate. |

| System and Information Integrity (SI) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| ***PISP Sec. 4.17.5*** | | personnel. | |
| **SI-6**<br>**Security Functionality Verification**<br><br>***PISP Sec. 4.17.6*** | Not required. | Not required. | 0 – 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.<br><br>1 – Employ automated mechanisms to provide centralized notification of failed automated security tests.<br><br>2 – Employ automated mechanisms to support centralized management of distributed security testing. |
| **SI-7**<br>**Software and** | Not Required. | 0 – Employ off-the-shelf integrity mechanisms such as parity checks, | 0 – Same as Moderate. |

| System and Information Integrity (SI) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Information Integrity**<br><br>***PISP Sec. 4.17.7*** | | 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. | 1 – Perform weekly integrity scans of the system.<br><br>2 – Employ automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification. |
| **SI-8**<br>**Spam Protection**<br><br>***PISP Sec. 4.17.8*** | No additional controls required beyond the referenced policy. | 1 – Centrally manage spam protection mechanisms. | 1 – Same as Moderate.<br><br>2 – Automatically update spam protection mechanisms. |
| **SI-9**<br>**Information Input Restrictions**<br><br>***PISP Sec. 4.17.9*** | Not required. | No additional controls required beyond the referenced policy. | No additional controls required beyond the referenced policy. |
| **SI-10** | Not required. | CMS-1 – Implement automated | CMS-1 – Same as Moderate. |

| System and Information Integrity (SI) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| **Information Accuracy, Completeness, Validity, and Authenticity**<br><br>***PISP Sec. 4.17.10*** | | system checks of information for accuracy, completeness, validity, and authenticity. | |
| **SI-11**<br>**Error Handling**<br><br>***PISP Sec. 4.17.11*** | Not Required. | 0 – 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. | 0 – Same as Moderate. |
| **SI-12**<br>**Information Output Handling and Retention** | 1 – Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information | 1– Same as Low. | 1 – Same as Low. |

| System and Information Integrity (SI) Standards | System Security Level Low | System Security Level Moderate | System Security Level High |
|---|---|---|---|
| ***PISP Sec. 4.17.12*** | system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements. | | |

**This page intentionally left blank**

# APPENDIX A – E-AUTHENTICATION STANDARDS

## INTRODUCTION

This appendix contains a broad set of CMS standards based upon National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, *Electronic Authentication Guideline*, V1.0.2, dated April 2006. It provides technical guidance to CMS to allow an individual person to remotely authenticate his/her identity to a CMS information system.

## PURPOSE

Federal Information Systems are required to incorporate information security controls to protect the information systems supporting their operations and missions. CMS is required to ensure the adequate protection of its information assets and must meet a minimum level of information security. NIST SP 800-63 supplements OMB guidance, *E-Authentication Guidance for Federal Agencies*, [OMB 04-04] and defines four (4) levels of assurance for electronic transactions, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. NIST SP 800-63 states specific technical requirements for each of the four (4) levels of assurance.

This document covers remote electronic authentication of human users to CMS information systems over a network. However, it does not address the authentication of a person who is physically present, for example for access to buildings, although some credentials and tokens that are used remotely may also be used for local authentication. Further, this document does not specifically address device-to-device (such as router-to-router) authentication, nor does it establish specific requirements for issuing authentication credentials and tokens to devices and servers when they are used in e-authentication protocols with people.

This document identifies minimum technical requirements for authenticating identity remotely. Business Owners can determine that additional measures are appropriate in certain contexts, based on their risk analysis. In particular, privacy requirements and legal risks may lead Business Owners to determine that additional authentication measures or other process safeguards are appropriate.

## E-AUTHENTICATION MODEL

In accordance with OMB guidance [OMB 04-04], e-authentication is the process of establishing confidence in user identities presented electronically to an information system. Systems can use the authenticated identity to determine whether that individual is authorized to perform an electronic transaction. In most cases, the authentications and transactions take place across an open network, such as the Internet. However, in some cases access to the network may be limited and access control decisions may take this into account.

E-authentication begins with registration. An applicant applies to a Registration Authority to become a subscriber of a Credential Service Provider (CSP) and, as a subscriber, is issued or

registers a secret, called a *token*, and a *credential* that binds the token to a name and possibly other attributes that the Registration Authority has verified. The token and credential may be used in subsequent authentication events.

In a common case, the Registration Authority and CSP are separate functions of the same system. However, a Registration Authority might be part of an organization that registers subscribers with an independent CSP, or several different CSPs. Therefore a CSP may have an integral Registration Authority, or it may have relationships with multiple independent Registration Authorities, and a Registration Authority may have relationships with different CSPs as well.

The subscriber's name may either be a verified name or a pseudonym. A verified name is associated with the identity of a real person. Before an applicant can receive credentials or register a token associated with a verified name, he/she must demonstrate that the identity is authentic, and that he/she is the person who is entitled to use that identity. This process is called *identity proofing*, and is performed by a Registration Authority that registers subscribers with the CSP.

At Level 1, since names are not verified, names are always assumed to be pseudonyms. Level 2 credentials and assertions must specify whether the name is a verified name or a pseudonym. This information assists parties who rely on the name or other authenticated attributes, in making access control or authorization decisions. Only verified names are allowed at Levels 3 and 4.

In summary, first an individual applicant applies to a Registration Authority. The Registration Authority identity proofs that applicant. As the result of successful identity proofing, the applicant becomes a subscriber of a CSP associated with the Registration Authority, with a credential and a secret token registered to the subscriber. When the subscriber needs to authenticate to perform a transaction, he/she becomes a claimant to a verifier. The claimant proves to the verifier that s/he controls the token, using an authentication protocol. If the verifier is separate from the relying party (application), the verifier provides an assertion about the claimant to the relying party, which uses the information in the assertion to make an access control or authorization decision. If the transaction is significant, the relying party may log the subscriber identity and credential(s) used in the authentication along with relevant transaction data.

**Table 5: E-Authentication Standards Definitions and Abbreviations**

| | |
|---|---|
| Address of Record | The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number, or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available. |
| Attack | An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possess a claimant's token. |
| Attacker | Party who is not the claimant or verifier but who wishes to execute the authentication protocol successfully as a claimant. |
| Approved | FIPS approved or NIST recommended. An algorithm or technique that is either:<br>1) specified in a FIPS or NIST Recommendation; or<br>2) adopted in a FIPS or NIST Recommendation.<br>Approved cryptographic algorithms must be implemented in a crypto module validated under FIPS 140-2 (as amended). For more information on validation and a list of validated FIPS 140-2 validated crypto modules see: http://csrc.nist.gov/cryptval/. |
| Assertion | A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol. |
| Asymmetric Keys | Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption, or signature generation and signature verification. |
| Authentication | The process of establishing confidence in user identities. |
| Authentication Protocol | A well-specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected. |
| Authenticity | The quality of data integrity that originates from its purported source. |
| Bit | A binary digit: 0 or 1. |
| Biometric | An image or template of a physiological attribute (e.g., a fingerprint) that may be used to identify an individual. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration. |
| Certification Authority (CA) | A trusted entity that issues and revokes public key certificates. |
| Certificate Revocation List (CRL) | A list of revoked public key certificates created and signed digitally by a Certification Authority. See [RFC 3280] |

| | |
|---|---|
| Challenge-Response Protocol | An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and independently can compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have authenticated himself successfully. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack. |
| Claimant | A party whose identity is to be verified using an authentication protocol. |
| Credential | An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. |
| Credentials Service Provider (CSP) | A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use. |
| Cryptographic Key | A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number. See also Asymmetric keys, Symmetric key. |
| Cryptographic Strength | A measure of the expected number of operations required to defeat a cryptographic mechanism. For the purposes of this document, this term is defined as meaning that breaking or reversing an operation is at least as difficult computationally as finding the key of an 80-bit block cipher by key exhaustion (it requires at least on the order of $2^{79}$ operations). |
| Cryptographic Token | A token where the secret is a cryptographic key. |
| Data Integrity | The property that data has not been altered by an unauthorized entity. |
| Digital Signature | An asymmetric key operation where the private key is used digitally to sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. |
| Electronic Credentials | Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document distinguishes between credentials, and tokens (see below) while other documents may interchange these terms. |
| Entropy | A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. |
| FIPS | Federal Information Processing Standard. |

| | |
|---|---|
| Guessing Entropy | A measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution. |
| Hash Function | A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:<br>1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and<br>2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output. |
| HMAC | Hash-based Message Authentication Code: a symmetric key authentication method using hash functions. |
| Identity | A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique. |
| Identity Proofing | The process by which a CSP and a Registration Authority validate sufficient information to uniquely identify a person. |
| Kerberos | A widely used authentication protocol developed at MIT. In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to-KDC exchange. |
| Man-in-the-Middle Attack (MitM) | An attack on the authentication protocol run in which the attacker is positioned between the claimant and verifier so that he/she can intercept and alter data traveling between them. |
| Message Authentication Code (MAC) | A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. |
| Min-Entropy | A measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system. When a password has n-bits of min-entropy then an attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The attacker is assumed to know the most commonly used password(s). |
| Network | An open communications medium, typically the Internet, which is used to transport messages between the claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party). |

| | |
|---|---|
| Nonce | A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement from a random challenge, because a nonce is not necessarily unpredictable. |
| Off-line Attack | An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing. |
| On-line Attack | An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets. |
| On-Line Certificate Status Protocol (OCSP) | An on-line protocol used to determine the status of a public key certificate. See [RFC 2560]. |
| Passive Attack | An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e. eavesdropping). |
| Password | A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. |
| Possession and Control of a Token | The ability to activate and use the token in an authentication protocol. |
| Personal Identification Number (PIN) | A password consisting only of decimal digits. |
| Practice Statement | A formal statement of the practices followed by an authentication entity (e.g., Registration Authority, CSP, or verifier); typically, the specific steps taken to register and verify identities, issue credentials, and authenticate claimants. |
| Private Key | The secret part of an asymmetric key pair that typically is used to digitally sign or decrypt data. |
| Proof of Possession (PoP) Protocol | A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password). |
| Protocol Run | An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant. |
| Public Key | The public part of an asymmetric key pair that typically is used to verify signatures or encrypt data. |
| Public Key Certificate | A digital document issued and signed digitally 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. See [RFC 3280] |

| | |
|---|---|
| Pseudonym | A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing. |
| Registration | The process through which a party applies to become a subscriber of a CSP and a Registration Authority validates the identity of that party on behalf of the CSP. |
| Registration Authority | A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The Registration Authority may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s). |
| Relying Party | An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system. |
| Salt | A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker. |
| Security Assertion Markup Language (SAML) | A specification for encoding security assertions in the XML markup language. |
| Shared Secret | A secret used in authentication that is known to the claimant and the verifier. |
| Subject | The person whose identity is bound in a particular credential. |
| Subscriber | A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol. |
| Symmetric Key | A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. |
| Token | Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity. |
| Transport Layer Security (TLS) | An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is similar to the older Secure Socket Layer (SSL) protocol and is effectively SSL version 3.1. |
| Tunneled Password Protocol | A protocol where a password is sent through a protected channel. For example, the TLS protocol is often used with a verifier's public key certificate to:<br>(1) authenticate the verifier to the claimant;<br>(2) establish an encrypted session between the verifier and claimant; and<br>(3) transmit the claimant's password to the verifier.<br>The encrypted TLS session protects the claimant's password from eavesdroppers. |
| Verified Name | A subscriber name that has been verified by identity proofing. |
| Verifier | An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status. |
| Verifier Impersonation Attack | An attack where the attacker impersonates the verifier in an authentication protocol, usually to learn a password. |

| | |
|---|---|
| Zero Knowledge Password | Strong password used with special “zero knowledge” protocol |
| Zero Knowledge Protocol | With Zero-knowledge protocols, someone can convince the verifier that he/she is in possession of the secret without revealing the secret itself, unlike normal username-password queries. |

# TECHNICAL REQUIREMENTS BY ASSURANCE LEVEL

## Registration and Identity Proofing

In the registration process an applicant undergoes identity proofing by a trusted Registration Authority. If the Registration Authority is able to verify the applicant's identity, the CSP registers or gives the applicant a token and issues a credential as needed to bind that token to the identity or some related attribute. The applicant is now a subscriber of the CSP and may use the token as a claimant in an authentication protocol.

Depending on the assurance level, the registration and identity proofing process is designed to ensure that the Registration Authority / CSP know the true identity of the applicant. Specifically, the requirements include measures to ensure that:

- A person with the applicant's claimed attributes exists, and those attributes are sufficient to identify a single person uniquely;
- The applicant whose token is registered is in fact the person who is entitled to the identity; and
- The applicant cannot later repudiate the registration; therefore, if there is a dispute later about an authentication using the subscriber's token, the subscriber cannot successfully deny he/she registered that token.

In some context, Business Owners may choose to use additional knowledge-based authentication methods to increase their confidence in the registration process. For example, an applicant could be asked to supply non-public information on his or her past dealing with CMS that could help confirm the applicant's identity.

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| **1. Registration Requirements** | There are no level-specific requirements at Level 1. | Both in-person and remote registration are permitted.<br><br>The applicant must supply his or her full | Both in-person and remote registration are permitted.<br><br>The applicant must supply his or her full | Only in-person registration is permitted.<br><br>The applicant must supply his or her full |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS requirements. | legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS requirements. | legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS requirements. |
| **2. Identity Proofing requirements** | | | | |
| **2.1. Basis for Issuing Credentials (In-Person)** | There are no level-specific requirements at Level 1. | Possession of a valid current primary Government Picture ID (e.g., driver's license or passport) that contains applicant's picture, and either address of record or nationality | Possession of verified current primary Government Picture ID (e.g., driver's license or passport) that contains applicant's picture and either address of record or nationality | In-person appearance and verification of two (2) independent ID documents or accounts, meeting the requirements of Level 3 (in-person and remote), one of which must be current primary Government Picture ID (e.g., driver's license or passport) that contains applicant's picture, and either address of record or nationality, and a |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | | | new recording of a biometric of the applicant at the time of application. |
| **2.2. Registration Authority Actions (In-Person)** | There are no level-specific requirements at Level 1. | Inspect photo-ID, compare picture to applicant, record ID number, address, and date of birth (DoB).<br><br>If ID appears valid and photo matches applicant then:<br>a) If ID confirms address of record, authorize or issue credentials, and send notice to address of record, or;<br>b) If ID does not confirm address of record, issue credentials in a manner that | Inspect Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases.<br><br>Confirm that: name, DoB, address, and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address, and DoB.<br><br>If ID is valid and photo matches applicant then:<br>a) If ID confirms address of record, authorize or issue | ***Primary Photo ID:*** Inspect Photo-ID and verify via the issuing government agency, compare picture to applicant, record ID number, address, and DoB.<br><br>***Secondary Government ID or financial account:***<br>a) Inspect Photo-ID and if apparently valid, compare picture to applicant, record ID number, address, and DoB, or;<br>b) Verify financial account number |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | confirms address of record. | credentials, and send notice to address of record, or;<br>b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record. | supplied by applicant through record checks or through credit bureaus or similar databases, and confirm that: name, DoB, address, and other personal information in records that are on balance consistent with the application and sufficient to identify a unique individual.<br><br>***Record Current Biometric:***<br>Record a current biometric (e.g., photograph or fingerprints to ensure that applicant cannot repudiate application. |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | | | ***Confirm Address:*** Issue credentials in a manner that confirms address of record. |
| **2.3. Basis for Issuing Credentials (Remote)** | There are no level-specific requirements at Level 1. | Possession of a valid Government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of **either** number. | Possession of a valid Government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of **both** numbers. | **Not Applicable** |
| **2.4. Registration Authority Actions (Remote)** | There are no level-specific requirements at Level 1. | Inspect both ID number and account number supplied by applicant. Verify information provided by applicant including ID number or account number through record checks either with the | Verify information provided by applicant including ID number and account number through record checks either with the applicable agency or institution, or through credit bureaus or | **Not applicable** |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | applicable agency or institution, or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.<br><br>Address confirmation and notification:<br>a) Send notice to an address of record confirmed in the records check or;<br>b) Issue credentials in a manner that confirms the address of record supplied by the applicant; or | similar databases, and confirms that: name, DoB, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual.<br><br>Address confirmation:<br>a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or<br>b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while | |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | c) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at a number or e-mail address associated with the applicant in records. | recording the applicant's voice. | |
| **3. Records Retention Requirements** | There are no level-specific requirements at Level 1. | A record of the facts of registration (including revocation) shall be maintained by the CSP or its representative.<br><br>The minimum record retention period for registration data is **seven (7) years and six (6) months beyond the expiration or revocation** (whichever is later) of the | A record of the facts of registration (including revocation) shall be maintained by the CSP or its representative.<br><br>The minimum record retention period for registration data is **seven (7) years and six (6) months beyond the expiration or revocation** (whichever is later) of the | A record of the facts of registration (including revocation) shall be maintained by the CSP or its representative.<br><br>The minimum record retention period for registration data is **ten (10) years and six (6) months beyond the expiration or revocation** (whichever is later) of the |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | credential. | credential. | credential. |
| **4. Federal PKI Certificate Policies** | There are no level-specific requirements at Level 1.<br><br>However, the Public Key Infrastructure (PKI) credentials are not limited to only those certificates by Certification Authorities (CA) cross-certified with the Federal Bridge CA. PKI credentials issued by any CA that has been determined to meet the identity proofing and registration requirements are permitted. | The identity proofing and certificate issuance processes of CAs cross-certified with the Federal Bridge CA (FBCA) under policies mapped to the Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate policies are deemed to meet the identity proofing provisions of this level.<br><br>However, the PKI credentials are not limited to only those certificates by CAs cross-certified with the FBCA. PKI credentials issued by any CA that has been determined to meet the identity | The identity proofing and certificate issuance processes of CAs cross-certified with the FBCA under policies mapped to the Basic, Medium, Medium-HW, or High Certificate polices are deemed to meet the identity proofing provisions of this level.<br><br>The PKI credentials must be issued by a CA cross-certified with the FBCA under one of the certificate policies identified above or a policy mapped to one of these policies.<br><br>However, a bi-directional cross- | The identity proofing and certificate issuance processes of CAs cross-certified with the FBCA under policies mapped to the Medium, Medium-HW, or High Certificate policies are deemed to meet the identity proofing provisions of this level.<br><br>The PKI credentials must be issued by a CA cross-certified with the FBCA under one of the certificate policies identified above or a policy mapped to one of these policies.<br><br>However, a bi-directional cross-certification is not |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | proofing and registration requirements are permitted. | certification is not required; it is sufficient that a valid certificate path exist from the Bridge CA to the issuing CA. The reverse certificate path need not exist. | required; it is sufficient that a valid certificate path exist from the Bridge CA to the issuing CA. The reverse certificate path need not exist. |

## Authentication Mechanism Requirements

This section covers the mechanical authentication process of a claimant who already has registered a token. The authentication process shall provide sufficient information to uniquely identify the registration information provided by the subscriber and verified by the Registration Authority in the issuance of the credential. The technical requirements for authentication mechanisms (tokens, protocols and security protections) are described in this section.

## Token

A token is something that the user possesses and controls (typically a key or password), and uses to authenticate the user's identity. Four (4) kinds of tokens for e-authentication are listed in this section. Each type of token incorporates one or more of the authentication factors (something you know, something you have, or something you are). Tokens that provide a higher level of assurance incorporate two or more factors. Tokens are included which focus upon the protection of critical systems. Unauthorized access frequently results in the compromise of system security and information confidentiality.

This recommendation requires multifactor authentication for e-Authentication Assurance Levels 3 and 4, and assigns tokens to the four (4) levels corresponding to the OMB guidance.

**NOTE:** When a control for a system is subject to higher standards to meet specific federal, legal, program, accounting, or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other higher standards.

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| **1. Tokens** | • On-line guessing<br>• Replay | • On-line guessing<br>• Replay<br>• Eavesdropper | • On-line guessing<br>• Replay<br>• Eavesdropper<br>• Verifier impersonation<br>• Man-in-the-Middle | • On-line guessing<br>• Replay<br>• Eavesdropper<br>• Verifier impersonation<br>• Man-in-the-Middle<br>• Session hijacking |
| **1.1. Passwords & PINs** | Employment of a wide range of available authentication technologies is allowed.<br><br>The use of any token methods of Levels 2, 3 or 4, as well as passwords is permitted.<br><br>Common protocols that meet the requirements include APOP [RFC | The use of any of the token methods of Levels 3 or 4, as well as passwords is permitted. | Passwords / PINs may be used as a second level authentication to unlock or use tokens. | Passwords / PINs may be used as a second level authentication to unlock or use tokens. |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | 1939], S/KEY [SKEY], and Kerberos [KERB]. | | | |
| **1.2. One-time Password Device Token** | The use of any of the methods of Level 3 is permitted. | The use of any of the methods of Level 3 is permitted. | If used, One-time Password Device Token shall meet the following requirements:<br>• The one-time password output by the device shall have at least $10^6$ possible values.<br>• Passwords must be generated randomly.<br>• The verifier must be authenticated cryptographically to the claimant, for example using a TLS server.<br>• To protect against the use of a stolen token, one of the following measures shall be used: | **Not Applicable** |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | | o The authentication mechanism used to authenticate the claimant to the token shall be validated as meeting the operator authentication requirements for FIPS 140-2 Level 2.<br>o The claimant must send the verifier a personal password meeting the requirements for (e-authentication) Level 1 with the one-time password. | |
| **1.3. Software Cryptography Token** (A cryptographic key | The use of any of the methods of Level 3 is permitted. | The use of any of the methods of Level 3 is permitted. | If used, Software tokens shall meet the following requirements: | **Not Applicable** |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| stored on a general-purpose computer.) | | | • The user shall be required to activate the key before using a TLS server.<br>• To protect against the use of a password as well as the key in an authentication protocol with the verifier.<br>• If a personal password meeting the requirements for (E-authentication), and decrypted only for actual use in authentication. Alternatively, if a password protocol is employed with the verifier, the use of the password shall meet the requirements for Level 2 | |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | | authentication assurance. | |
| **1.4. Hardware Cryptography Token** (A cryptographic key stored on a special hardware device) | The use of any of the methods of Level 3 is permitted. | The use of any of the methods of Level 3 is permitted. | If used, Hardware tokens shall meet the following requirements:<br>• Tokens must be validated at FIPS 140-2 Level 1 or higher overall.<br>• The user shall be required to activate the key before using it with a password or biometric, or, alternatively shall use a password as well as the key in an authentication protocol with the verifier.<br>• The authentication mechanism used to authenticate the claimant to unlock token shall be | Hardware tokens shall meet the following requirements:<br>• Token must be validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security.<br>• Requires the entry of a password or a biometric to activate the authentication key.<br>• Must not be able to export authentication keys. |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | | validated as meeting the operator authentication requirements for FIPS 140-2 Level 2.<br>• Alternatively, if a password protocol is employed with a verifier, the use of the password shall meet the requirements for Level 1 authentication assurance. | |
| **2. Credential / Token Lifetime, Status or Revocation** | The use of any of the methods of Levels 3 or 4 is permitted. | The use of any of the methods of Levels 3 or 4 is permitted. | CSPs shall have a procedure to revoke credentials and tokens within one (1) hour. | CSPs shall have a procedure to revoke credentials immediately after being notified that a credential is no longer valid or a token is compromised. |
| **3. Assertions** | Relying parties may accept assertions that are:<br>• Digitally signed by | Relying parties may accept assertions that are:<br>• Digitally signed by | Relying parties may accept assertions that are:<br>• Digitally signed by | N/A |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | a trusted entity (e.g., the verifier); or<br>• Obtained directly from a trusted entity (e.g., a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g., TLS) that cryptographically authenticates the verifier and protects the assertion. | a trusted entity (e.g., the verifier); or<br>• Obtained directly from a trusted entity (e.g., a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g., TLS) that cryptographically authenticates the verifier and protects the assertion.<br>• Assertions generated by a verifier shall expire after twelve (12) hours and should not be accepted thereafter by the | a trusted entity (e.g., the verifier); or<br>• Obtained directly from a trusted entity (e.g., a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g., TLS) that cryptographically authenticates the verifier and protects the assertion.<br>• Assertions generated by a verifier shall expire after two (2) hours and should not be accepted thereafter by the relying | |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | relying party. | party. | |
| **4. Protection of Long-Term Shared Secrets** | Files of shared secrets used by verifiers at Level 1 authentication shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such shared secret files shall not contain the plaintext passwords; typically they contain a one-way hash or "inversion" of the password.<br><br>In addition, any method allowed for the protection of long-term shared secrets at Levels 2, 3 or 4 may be used at Level 1. | Long-term shared authentication secrets, if used, shall never be revealed to any party except the subscriber and CSP, however session (temporary) shared secrets may be provided by the CSP to independent verifiers.<br><br>Files of shared secrets used by CSPs at Level 2 shall be protected by discretionary access controls that limit access to administrators and only those applications that require access.<br><br>Such shared secret files shall not contain the plaintext passwords or secret; two alternative | Files of long-term shared secrets used by CSPs or verifiers at Level 3 shall be protected by discretionary access controls that limit access to administrators and only those applications that require access.<br><br>Such shared secret files shall be encrypted so that:<br>1. The encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 | N/A |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | methods may be used to protect the shared secret:<br>1. Passwords may be concatenated to a salt and/or username and then hashed with an Approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file.<br>2. Store shared secrets in encrypted form using approved encryption algorithms and | cryptographic module and decrypted only as immediately required for an authentication operation.<br>2. Shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module, or any FIPS 140-2 Level 3, or 4 cryptographic modules, and is not exported in plaintext from the module.<br>3. Shared secrets are split by a cryptographic secret sharing method between *m* separate | |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | modes. Then decrypt the needed secret, when immediately required for authentication.<br><br>In addition any method protecting shared secrets, at Level 3 or 4 may be used at Level 2. | verifier systems, so that the cooperation of *n* (where $2 \leq n \leq m$) systems in a secure protocol is required to perform the authentication and an attacker who learns *n-1* of the secret shares, learns nothing about the secret (except, perhaps, its size). | |

## SUMMARY OF TECHNICAL REQUIREMENTS

This section summarizes the technical requirements for each level. Table 6 lists the types of tokens that may be used at each assurance level. Table 7 identifies the protections that are required at each level. Table 8 identifies the types of authentication protocols that are applicable to each assurance level. Table 9 identifies additional required protocol and system properties at each level.

**Table 6: Token Types Allowed at Each Assurance Level**

| Token Type | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| Hard crypto token | √ | √ | √ | √ |
| One-time password device | √ | √ | √ | |
| Soft crypto token | √ | √ | √ | |
| Passwords & PINs | √ | √ | | |

**Table 7: Required Protections**

| Exploits | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| On-line guessing | √ | √ | √ | √ |
| Replay | √ | √ | √ | √ |
| Eavesdropper | | √ | √ | √ |
| Verifier impersonation | | | √ | √ |
| Man-in-the-middle | | | √ | √ |

| | | | | |
|---|---|---|---|---|
| Session hijacking | | | | √ |

**Table 8: Authentication Protocol Types**

| Protocol Type | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| Private Key PoP | √ | √ | √ | √ |
| Symmetric key PoP | √ | √ | √ | √ |
| Tunneled Password or Zero knowledge password | √ | √ | | |
| Challenge-reply Password | √ | | | |

**Table 9: Additional Required Properties**

| Required Property | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| Shared secrets not revealed to third parties by verifiers or CSPs | | √ | √ | √ |
| Multi-factor authentication | | | √ | √ |
| Sensitive data transfer authenticated | | | | √ |

# APPENDIX B – STANDARDS FAMILY CLASSIFICATION

Security standards in the ARS (Sections 1 through 17) have a well-defined organization and structure. The standards are organized alphabetically by the family identifier for ease of use in selection for the specification process. However, there are three (3) general classes of security standards (i.e., Management, Operational, and Technical), which correspond to the major sections of a SSP. Each class contains control families related to the function of the class. Each family was established by NIST SP 800-53 which named them, "security control families" and assigned unique two-character identifiers to each control family. Table 10 summarizes the classes and families in the ARS and the associated family identifiers by class for cross reference purposes the SSP standard.

**Table 10: Families by Class**

| Class | Family | Identifier |
|---|---|---|
| Management | Certification, Accreditation, and Security Assessments | CA |
| Management | Planning | PL |
| Management | Risk Assessments | RA |
| Management | System and Services Acquisition | SA |
| Operational | Awareness and Training | AT |
| Operational | Configuration Management | CM |
| Operational | Contingency Planning | CP |
| Operational | Incident Response | IR |
| Operational | Maintenance | MA |
| Operational | Media Protection | MP |
| Operational | Physical and Environmental Protection | PE |
| Operational | Personnel Security | PS |
| Operational | System and Information Integrity | SI |
| Technical | Access Control | AC |
| Technical | Audit and Accountability | AU |
| Technical | Identification and Authentication | IA |
| Technical | System and Communications Protection | SC |

# APPENDIX C – HISTORICAL LOG OF STANDARDS REDISTRIBUTION

## Table 11: ARS V3.0 Redistribution

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| ***ARS v2.0 Category:*** | ***AC – Access Control*** | ***AC – Access Control*** |
| AC-2.4 | Account Management | Revised for clarity; added 800-53r1 Moderate control |
| AC-3.CMS-1 | Access Enforcement | Revised for clarity |
| AC-3.CMS-2 | Access Enforcement | Revised ARS Appendix C reference for clarity and consistency |
| AC-3.CMS-3 | Access Enforcement | Removed; control included in AC-3.1 |
| AC-3.CMS-4 | Access Enforcement | Renumbered to AC-3.CMS-3 |
| AC-3.CMS-5 | Access Enforcement | Renumbered to AC-3.CMS-4 |
| AC-3.1 | Access Enforcement | Revised to incorporate AC-3.CMS-3 and CM-5.CMS-1 controls |
| AC-4 | Information Flow Enforcement | Revised for clarity |
| AC-4.CMS-1 | Information Flow Enforcement | Removed; control included in SC-7.5 |
| AC-4.CMS-2 | Information Flow Enforcement | Removed; control included in SC-9 |
| AC-5.CMS-5 | Separation of Duties | Revised "Business Owner" term |
| AC-6.CMS-1 | Least Privilege | Removed; control included in AC-3.1 |
| AC-6.CMS-2 | Least Privilege | Renumbered to AC-6.CMS-1 |
| AC-6.CMS-3 | Least Privilege | Renumbered to AC-6.CMS-2 |
| AC-6.CMS-4 | Least Privilege | Renumbered to AC-6.CMS-3 |
| AC-6.CMS-5 | Least Privilege | Renumbered to AC-6.CMS-4 |
| AC-8.CMS-1 | System Use Notification | Replaced bullets for clarity |
| AC-8.CMS-2 | System Use Notification | Revised for clarity |
| AC-8.CMS-3 | System Use Notification | Removed; included in PISP |
| AC-8.CMS-~~4~~ | System Use Notification | Renumbered to AC-8.CMS-3 |
| AC-10.0 | Concurrent Session Control | Revised for clarity and to specify allowed number of network log-on sessions |
| AC-11.0 | Session Lock | Revised for clarity |
| AC-12.0 | Session Termination | Revised for 800-53r1 |
| AC-13.1 | Supervision and Review – Access Control | Added control to Moderate |
| AC-16.CMS-1 | Automated Labeling | Revised punctuation |
| AC-17.CMS-1 | Remote Access | Revised for 800-53r1 and clarity |
| AC-17.CMS-3 | Remote Access | Revised for clarity |
| AC-17.CMS-4 | Remote Access | Revised ARS Appendix A reference |

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| | | for clarity and consistency |
| AC-17.2 | Remote Access | Revised for 800-53r1 |
| AC-17.3 | Remote Access | Revised for 800-53r1 and added control to Moderate |
| AC-18.0 | Wireless Access Restrictions | Renumbered for consistency and revised for clarity |
| AC-19.1 | Access Control for Portable and Mobile Devices | Revised 800-53r1 security control name, and revised for 800-53r1 and clarity |
| AC-20.0 | Personally-Owned Information Systems | Revised 800-53r1 security control name, and control removed; included in PISP |
| AC-CMS-1.CMS-1 | System Boot Access | Revised for clarity |
| AC-CMS-1.CMS-2 | System Boot Access | Revised for clarity |
| AC-CMS-1.CMS-3 | System Boot Access | Revised for clarity |
| ***ARS V2.0 Category*** | ***AT – Awareness and Training*** | ***AT – Awareness and Training*** |
| AT-2.0 | Security Awareness | Revised for 800-53r1 and clarity |
| AT-3.0 | Security Training | Revised for 800-53r1 |
| ***ARS V2.0 Category:*** | ***AU – Audit and Accountability*** | ***AU – Audit and Accountability*** |
| AU-2.0 | Auditable Events | Replaced bullets for clarity |
| AU-2.CMS-1 | Auditable Events | Punctuation change |
| AU-4 | Audit Storage Capacity | Removed; moved High control to new 800-53r1 AU-5.1 and AU-5.2 controls |
| AU-5.0 | Audit Processing | Revised 800-53r1 security control name and replaced bullets for clarity |
| AU-6.CMS-1 | Audit Monitoring, Analysis, and Reporting | Revised for 800-53r1 |
| AU-6.CMS-4 | Audit Monitoring, Analysis, and Reporting | Revised for 800-53r1 |
| AU-6.CMS-6 | Audit Monitoring, Analysis, and Reporting | Revised for 800-53r1 |
| AU-6.2 | Audit Monitoring, Analysis, and Reporting | Revised for 800-53r1; added control to Moderate |
| AU-11.0 | Audit Retention | Revised 800-53r1 security control name and revised for 800-53r1 |
| ***ARS V2.0 Category:*** | ***CA – Certification, Accreditation, and Security Assessments*** | ***CA – Certification, Accreditation, and Security Assessments*** |
| CA-3.CMS-1 | Information System Connections | Revised 800-53r1 security control name |
| CA-4.CMS-1 | Security Certification | Revised for clarity |
| CA-5.0 | Plan of Action and Milestones | Revised for clarity and to specify |

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| | | timeframe for POA&M creation |
| CA-7.CMS-1 | Continuous Monitoring | Replaced bullets for clarity |
| CA-CMS-1.CMS-1 | Information Security Business Risk Assessment | Removed; CA-CMS-1.CMS-1 control merged with RA-3 control |
| ***ARS V2.0 Category:*** | ***CM – Configuration Management*** | ***CM – Configuration Management*** |
| CM-2.CMS-1 | Baseline Configuration | Revised for 800-53r1 and to specify review as annual requirement |
| CM-2.1 | Baseline Configuration | Revised for 800-53r1 |
| CM-2.2 | Baseline Configuration | Revised for 800-53r1 |
| CM-3.1 | Configuration Change Control | Replaced bullets for clarity |
| CM-4.CMS-1 | Monitoring Change Activity | Revised 800-53r1 security control name |
| CM-5.CMS-1 | Access Restrictions for Change | Removed; control merged with AC-3.1 |
| CM-6.1 | Configuration Settings | Revised punctuation |
| CM-7.0 | Least Functionality | Replaced bullets for clarity |
| ***ARS V2.0 Category:*** | ***CP – Contingency Planning*** | ***CP – Contingency Planning*** |
| CP-3.0 | Contingency Training | Revised for clarity |
| CP-4.0 | Contingency Plan Testing | Revised 800-53r1 security control name and for punctuation |
| CP-4.1 | Contingency Plan Testing | Revised for 800-53r1 and replaced bullets for clarity |
| CP-4.2 | Contingency Plan Testing | Revised for 800-53r1 |
| CP-4.3 | Contingency Plan Testing | Revised for 800-53r1 |
| CP-5.0 | Contingency Plan Update | Revised for clarity |
| CP-6 | Alternate Storage Sites | Revised 800-53r1 security control name |
| CP-6.1 | Alternate Storage Sites | Removed 100-mile distance control |
| CP-6.3 | Alternate Storage Sites | Control added Moderate to be consistent with CP-7 control |
| CP-7.0 | Alternate Processing Sites | Revised 800-53r1 security control name and added HSPD-20 requirement to provide different Recovery Time Objectives (RTO) for Moderate and High |
| CP-7.1 | Alternate Processing Sites | Removed 100-mile distance control |
| CP-8.0 | Telecommunications Services | Revised for HSPD-20 requirement to provide different Recovery Time Objectives (RTO) for Moderate and High |
| CP-8.4 | Telecommunications Services | Revised for 800-53r1 |

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| CP-9.0 | Information System Backups | Revised 800-53r1 security control name, and revised for clarity and to integrate ARS MP-4.CMS-1 and MP-4.CMS2 controls |
| CP-9.1 | Information System Backups | Revised for 800-53r1 |
| CP-10.0 | Information System Recovery and Reconstitution | Punctuation and replaced bullets for clarity |
| ***ARS V2.0 Category:*** | ***IA – Identification and Authentication*** | ***IA – Identification and Authentication*** |
| IA-2.1 | User Identification and Authentication | Revised for 800-53r1; High control changed to Moderate-only control |
| IA-3.0 | Device and Host Identification and Authentication | Revised 800-53r1 security control name |
| IA-4.0 | Identifier Management | Revised timeframe for consistency |
| IA-4.CMS-1 | Identifier Management | Revised punctuation |
| IA-5.0 | Authenticator Management | Revised ARS Appendix A reference for clarity and consistency, and replaced bullets for clarity |
| IA-6.0 | Authenticator Feedback | Revised punctuation |
| IA-7.0 | Cryptographic Module Authentication | Former wording did not deal with authentication to a Cryptographic module - ref FIPS 140-2 section 4.3.3 |
| IA.CMS-1 | Help Desk Support Procedures | Removed; moved to IA-2.CMS-3 |
| ***ARS V2.0 Category:*** | ***IR – Incident Response*** | ***IR – Incident Response*** |
| IR-3.0 | Incident Response Testing | Revised 800-53r1 security control name and revised for 800-53r1 |
| IR-3.1 | Incident Response Testing | Revised for 800-53r1 |
| IR-4.CMS-1 | Incident Handling | Revised to specify proper title |
| ***ARS V2.0 Category:*** | ***MA – Maintenance*** | ***MA – Maintenance*** |
| MA-2.0 | Periodic Maintenance | Revised 800-53r1 security control name and base control removed; included in PISP. Removed Moderate and High add-on controls, and controls included in ARS SI-2 and SI-3.1. |
| MA-2.1 | Periodic Maintenance | Revised for 800-53r1 and removed Low control; revised bullets for clarity |
| MA-2.2 | Periodic Maintenance | Revised for 800-53r1 |
| MA-3.2 | Maintenance Tools | Revised for 800-53r1 |
| MA-3.4 | Maintenance Tools | Revised for 800-53r1 |
| MA-4.1 | Remote Maintenance | Revised for 800-53r1 and added control to Moderate |

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| MA-4.2 | Remote Maintenance | Added control to Moderate |
| MA-4.3 | Remote Maintenance | Revised for 800-53r1 and to include MA-4.0 High add-on control |
| MA-4.0 | Remote Maintenance | Renumbered as MA-4.CMS-1 and removed MA-4.0 High add-on control which is included in new 800-53r1 MA-4.3 control |
| MA-5.0 | Maintenance Personnel | Revised for consistency |
| MA-CMS-1.CMS-1 | Off-site Physical Repair of Systems | Revised for clarity |
| MA-CMS-2.CMS-1 | On-site Physical Repair of Systems | MA-CMS-2.CMS-2 Moderate and High controls changed to MA-CMS-2.CMS-1 to match Low control |
| MA-CMS-2.CMS-2 | On-site Physical Repair of Systems | MA-CMS-2.CMS-1 Moderate and High controls changed to MA-CMS-2.CMS-2 due to above renumbering |
| ***ARS V2.0 Category:*** | ***MP – Media Protection*** | ***MP – Media Protection*** |
| MP-2.1 | Media Access | Revised for 800-53r1 and added control to Moderate |
| MP-3.0 | Media Labeling | Renumbered and control removed; included in PISP. |
| MP-3.CMS-1 | Media Labeling | Revised for clarity |
| MP-4 | Media Storage | Revised for consistency |
| MP-4.CMS-1 | Media Storage | Removed; control moved to CP-9 |
| MP-4.CMS-2 | Media Storage | Removed; control moved to CP-9 |
| MP-4.CMS-3 | Media Storage | Removed; included in PISP |
| MP-4.CMS-4 | Media Storage | Removed; merged with MP-5.1 |
| MP-5 | Media Transport | Revised for 800-53r1 |
| MP-6.0 | Media Sanitization | Revised 800-53r1 security control name, and revised for clarity and to incorporate MP-7.CMS-1 and MP-7.CMS-2 controls |
| MP-7.CMS-1 | Media Destruction and Disposal | Removed; 800-53r1 control deleted and merged w/MP-6. Former ARS MP-7.CMS-1 controls added to ARS MP-6.0. |
| MP-7.CMS-2 | Media Destruction and Disposal | Removed; 800-53r1 control deleted and merged w/MP-6. Former ARS MP-7.CMS-2 controls added to ARS MP-6.0. |
| MP-CMS-1 | Media Related Records | Replaced bullets and revised for clarity, and to specify records must allow for reconstruction of the data, if necessary |

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| ***ARS V2.0 Category:*** | ***PE – Physical and Environmental Protection*** | ***PE – Physical and Environmental Protection*** |
| PE-3.CMS-1 | Physical Access Control | Revised for clarity (i.e., data centers include all computing centers not only mainframe centers). |
| PE-3.CMS-2 | Physical Access Control | Renumbered to PE-3.CMS-4 and removed Low control; included in PISP |
| PE-3.CMS-3 | Physical Access Control | Renumbered to PE-3.CMS-2 and revised for clarity |
| PE-3.CMS-4 | Physical Access Control | Renumbered to PE-3.CMS-3 and revised for clarity (i.e., data centers include all computing centers not only mainframe centers). |
| PE-4.CMS-1 | Access Control for Transmission Media | Revised for 800-53r1 and clarity |
| PE-5.0 | Access Control for Display Medium | Renumbered for consistency and removed control; included in PISP |
| PE-6.1 | Monitoring Physical Access | Revised for 800-53r1 |
| PE-6.2 | Monitoring Physical Access | Revised for clarity |
| PE-8.0 | Access Logs | Revised 800-53r1 security control name, and revised control for clarity |
| PE-8.1 | Access Logs | Removed Moderate control |
| PE-10.CMS-1 | Emergency Shutoff | Revised for clarity (i.e., data centers include all computing centers not only mainframe centers). |
| PE-13.1 | Fire Protection | Revised for 800-53r1 |
| PE-13.2 | Fire Protection | Revised for 800-53r1 and control added to Moderate |
| PE-14.CMS-1 | Temperature and Humidity Controls | Revised for clarity |
| PE-15.1 | Water Damage Protection | Revised for clarity |
| PE-17.CMS-1 | Alternate Worksite | Revised 800-53r1 security control name |
| PE-CMS-1.CMS-1 | Power Surge Protection | Removed; control moved to PE-9.CMS-2 |
| PE-CMS-2.CMS-1 | Physical Ports | Removed; control moved to PE-4.CMS-2 |
| PE-CMS-3.CMS-1 | Restrict the Use of Portable Computing Devices | Removed; control included in AC-19 |
| ***ARS V2.0 Category:*** | ***PL – Planning*** | ***PL – Planning*** |
| PL-2.CMS-1 | System Security Plan | Revised for clarity |
| PL-4.CMS-2 | Rules of Behavior | Revised for clarity |
| ***ARS V2.0 Category:*** | ***PS – Personnel Security*** | ***PS – Personnel Security*** |

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| PS-6.0 | Access Agreements | Revised for 800-53r1 and clarity |
| PS-CMS-1.CMS-1 | Review System Access during Extraordinary Personnel Circumstances | Revised for clarity |
| ***ARS V2.0 Category:*** | ***RA – Risk Assessments*** | ***RA – Risk Assessments*** |
| RA-3.CMS-1 | Risk Assessments (RA) | Revised 800-53r1 security control name and merged CA-CMS-1.CMS-1 control |
| RA-3.CMS-2 | Risk Assessments (RA) | Removed; control moved to CA-5.CMS-1 |
| RA-4 | Risk Assessments Update | Revised 800-53r1 security control name |
| RA-5.0 | Vulnerability Scanning | Added "Not Required" to Low for consistency |
| RA-5.2 | Vulnerability Scanning | Revised for 800-53r1 |
| ***ARS V2.0 Category:*** | ***SA – System and Services Acquisition*** | ***SA – System and Services Acquisition*** |
| SA-4.CMS-1 | Acquisitions | Revised punctuation |
| SA-8.0 | Security Design Principles | Revised 800-53r1 security control name |
| SA-9.0 | Outsourced Information System Services | Revised 800-53r1 security control name and revised for clarity; renumbered for consistency |
| SA-11 | Developer Security Testing | Revised for punctuation and renumbered for consistency |
| ***ARS V2.0 Category:*** | ***SC – Systems and Communications Protection*** | ***SC – Systems and Communications Protection*** |
| SC-3.2 | Security Function Isolation | Revised for 800-53r1 |
| SC-3.3 | Security Function Isolation | Revised for 800-53r1 |
| SC-3.4 | Security Function Isolation | Revised for 800-53r1 |
| SC-3.5 | Security Function Isolation | Revised for 800-53r1 |
| SC-4.0 | Information Remnants | Revised 800-53r1 security control name |
| SC-5.0 | Denial-of-Service Protection | Replaced bullets and punctuation for clarity |
| SC-7.CMS-1 | Boundary Protection | Removed; moved to new 800-53r1 SC-7.5 control |
| SC-7.CMS-2 | Boundary Protection | Renumbered to SC-7.CMS-1 |
| SC-7.CMS-3 | Boundary Protection | Renumbered to SC-7.CMS-2 |
| SC-7.CMS-4 | Boundary Protection | Renumbered to SC-7.CMS-3 |
| SC-7.1 | Boundary Protection | Revised for clarity and consistency |
| SC-7.CMS-1 | Boundary Protection | New 800-53r1 enhancement; |

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| | | renumbered and moved former SC-7.CMS-1 control here |
| SC-8.CMS-1 | Transmission Integrity | Revised; encryption for confidentiality is addressed in SC-9.CMS-1. |
| SC-8.1 | Transmission Integrity | Revised for clarity and control added to Moderate for consistency (i.e., SC-8.CMS-1 is Moderate) |
| SC-9.CMS-1 | Transmission Confidentiality | Removed; replaced by revised SC-9.1 |
| SC-9.1 | Transmission Confidentiality | Revised for 800-53r1 and for clarity; control added to Moderate for consistency (i.e.,SC-9.CMS-1 is Moderate) |
| SC-10.0 | Network Disconnect | Revised punctuation |
| SC-10.CMS-1 | Network Disconnect | Removed; included in AC-11 |
| SC-10.CMS-2 | Network Disconnect | Removed; included in AC-11 |
| SC-11 | Trusted Path | Revised for 800-53r1 and renumbered to SC-11.0 for consistency |
| SC-12.CMS-1 | Cryptographic Key Management | Revised 800-53r1 security control name and revised for consistency |
| SC-13 | Use of Cryptography | Revised 800-53r1 security control name |
| SC-14.CMS-2 | Public Access Protections | Revised ARS Appendix A reference for clarity and consistency |
| SC-15.CMS-1 | Collaborative Computing | Revised for 800-53r1 and punctuation |
| SC-19.CMS-1 | Voice Over Internet Protocol | Changed acronym and revised for clarity |
| SC-CMS-2.CMS-1 | Identify and Detect Unauthorized Modems | Revised for clarity and punctuation |
| SC-CMS-3.CMS-1 | Secondary Authentication and Encryption | Revised punctuation and revised security mechanism |
| SC-CMS-3.CMS-2 | Secondary Authentication and Encryption | Revised ARS Appendix A reference for clarity and consistency |
| SC-CMS-4.CMS-1 | Electronic Mail | Revised for clarity |
| SC-CMS-5.CMS-1 | Persistent Cookies | Revised for clarity |
| ***ARS V2.0 Category:*** | ***SI – System and Information Integrity*** | ***SI – System and Information Integrity*** |
| SI-2.0 | Flaw Remediation | Replaced bullets for clarity |
| SI-2.1 | Flaw Remediation | Revised for 800-53r1 and clarity |
| SI-2.2 | Flaw Remediation | Revised for 800-53r1 |
| SI-3.CMS-1 | Malicious Code Protection | Revised for 800-53r1 |

| ARS 2.0 Standard No. | ARS 2.0 Standard Name | ARS 3.0 Redistribution |
|---|---|---|
| SI-3.1 | Malicious Code Protection | Revised for 800-53r1 |
| SI-3.2 | Malicious Code Protection | Revised for 800-53r1 |
| SI-4.CMS-1 | Intrusion Detection Tools and Techniques | Revised 800-53r1 security control name |
| SI-4.CMS-2 | Intrusion Detection Tools and Techniques | Removed; replaced by new 800-53r1 SI-4.5 control |
| SI-4.2 | Intrusion Detection Tools and Techniques | Revised for 800-53r1 |
| SI-4.4 | Intrusion Detection Tools and Techniques | Revised for 800-53r1 and added control Moderate |
| SI-5.1 | Security Alerts and Advisories | Revised for clarity |
| SI-6.1 | Security Functionality Verification | Revised for 800-53r1 |
| SI-8 | Spam and Spyware Protection | Revised 800-53r1 security control name |
| SI-8.1 | Spam and Spyware Protection | Revised for 800-53r1 |
| SI-8.2 | Spam and Spyware Protection | Revised for 800-53r1 |
| SI-10.CMS-1 | Information Input Accuracy, Completeness, and Validity | Revised 800-53r1 security control name and control for 800-53r1 |
| SI-12.1 | Information Output Handling and Retention | Revised for 800-53r1 and renumbered to SI-12.0 for consistency |

## Table 12: ARS V2.0 Redistribution

| ARS 1.2 Standard No. | ARS 1.2 Standard Name | ARS 1.2 Standards Category |
|---|---|---|
| ***ARS v2.0 Category:*** | ***AC – Access Control*** | ***AC – Access Control*** |
| AC-2.4 | Account Management | Revised for clarity; added 800-53r1 Moderate control |
| AC-3.CMS-1 | Access Enforcement | Revised for clarity |
| AC-3.CMS-2 | Access Enforcement | Revised ARS Appendix A reference for clarity and consistency |
| AC-3.CMS-3 | Access Enforcement | Removed; control included in AC-3.1 |
| AC-3.CMS-4 | Access Enforcement | Renumbered to AC-3.CMS-3 |
| AC-3.CMS-5 | Access Enforcement | Renumbered to AC-3.CMS-4 |
| AC-3.1 | Access Enforcement | Revised to incorporate AC-3.CMS-3 and CM-5.CMS-1 controls |
| AC-4 | Information Flow Enforcement | Revised for clarity |
| AC-4.CMS-1 | Information Flow Enforcement | Removed; control included in SC-7.5 |
| AC-4.CMS-2 | Information Flow Enforcement | Removed; control included in SC-9 |
| AC-5.CMS-5 | Separation of Duties | Revised "business owner" term |
| AC-6.CMS-1 | Least Privilege | Removed; control included in AC-3.1 |
| AC-6.CMS-2 | Least Privilege | Renumbered to AC-6.CMS-1 |
| AC-6.CMS-3 | Least Privilege | Renumbered to AC-6.CMS-2 |
| AC-6.CMS-4 | Least Privilege | Renumbered to AC-6.CMS-3 |
| AC-6.CMS-5 | Least Privilege | Renumbered to AC-6.CMS-4 |
| AC-8.CMS-1 | System Use Notification | Replaced bullets for clarity |
| AC-8.CMS-2 | System Use Notification | Revised for clarity |
| AC-8.CMS-3 | System Use Notification | Removed; included in PISP |
| AC-8.CMS-~~4~~ | System Use Notification | Renumbered to AC-8.CMS-3 |
| AC-10.0 | Concurrent Session Control | Revised for clarity and to specify allowed number of network log-on sessions |
| AC-11.0 | Session Lock | Revised for clarity |
| AC-12.0 | Session Termination | Revised for 800-53r1 |
| AC-13.1 | Supervision and Review – Access Control | Added control to Moderate |
| AC-16.CMS-1 | Automated Labeling | Revised punctuation |
| AC-17.CMS-1 | Remote Access | Revised for 800-53r1 and clarity |
| AC-17.CMS-3 | Remote Access | Revised for clarity |
| AC-17.CMS-4 | Remote Access | Revised ARS Appendix A reference for clarity and consistency |
| AC-17.2 | Remote Access | Revised for 800-53r1 |
| AC-17.3 | Remote Access | Revised for 800-53r1 and added control to Moderate |

| ARS 1.2 Standard No. | ARS 1.2 Standard Name | ARS 1.2 Standards Category |
|---|---|---|
| AC-18.0 | Wireless Access Restrictions | Renumbered for consistency and revised for clarity |
| AC-19.1 | Access Control for Portable and Mobile Devices | Revised 800-53r1 security control name, and revised for 800-53r1 and clarity |
| AC-20.0 | Personally-Owned Information Systems | Revised 800-53r1 security control name, and control removed; included in PISP |
| AC-CMS-1.CMS-1 | System Boot Access | Revised for clarity |
| AC-CMS-1.CMS-2 | System Boot Access | Revised for clarity |
| AC-CMS-1.CMS-3 | System Boot Access | Revised for clarity |
| ***ARS V2.0 Category:*** | ***AT – Awareness and Training*** | ***AT – Awareness and Training*** |
| AT-2.0 | Security Awareness | Revised for 800-53r1 and clarity |
| AT-3.0 | Security Training | Revised for 800-53r1 |
| ***ARS V2.0 Category:*** | ***AU – Audit and Accountability*** | ***AU – Audit and Accountability*** |
| AU-2.0 | Auditable Events | Replaced bullets for clarity |
| AU-2.CMS-1 | Auditable Events | Punctuation change |
| AU-4 | Audit Storage Capacity | Removed; moved High control to new 800-53r1 AU-5.1 and AU-5.2 controls |
| AU-5.0 | Audit Processing | Revised 800-53r1 security control name and replaced bullets for clarity |
| AU-6.CMS-1 | Audit Monitoring, Analysis, and Reporting | Revised for 800-53r1 |
| AU-6.CMS-4 | Audit Monitoring, Analysis, and Reporting | Revised for 800-53r1 |
| AU-6.CMS-6 | Audit Monitoring, Analysis, and Reporting | Revised for 800-53r1 |
| AU-6.2 | Audit Monitoring, Analysis, and Reporting | Revised for 800-53r1; added control to Moderate |
| AU-11.0 | Audit Retention | Revised 800-53r1 security control name and revised for 800-53r1 |
| ***ARS V2.0 Category:*** | ***CA – Certification, Accreditation, and Security Assessments*** | ***CA – Certification, Accreditation, and Security Assessments*** |
| CA-3.CMS-1 | Information System Connections | Revised 800-53r1 security control name |
| CA-4.CMS-1 | Security Certification | Revised for clarity |
| CA-5.0 | Plan of Action and Milestones | Revised for clarity and to specify timeframe for POA&M creation |
| CA-7.CMS-1 | Continuous Monitoring | Replaced bullets for clarity |

| | | |
|---|---|---|
| CA-CMS-1.CMS-1 | Information Security Business Risk Assessment | Removed; CA-CMS-1.CMS-1 control merged with RA-3 control |

| ARS 1.2 Standard No. | ARS 1.2 Standard Name | ARS 1.2 Standards Category |
|---|---|---|
| ***ARS V2.0 Category:*** | ***CM – Configuration Management*** | ***CM – Configuration Management*** |
| CM-2.CMS-1 | Baseline Configuration | Revised for 800-53r1 and to specify review as annual requirement |
| CM-2.1 | Baseline Configuration | Revised for 800-53r1 |
| CM-2.2 | Baseline Configuration | Revised for 800-53r1 |
| CM-3.1 | Configuration Change Control | Replaced bullets for clarity |
| CM-4.CMS-1 | Monitoring Change Activity | Revised 800-53r1 security control name |
| CM-5.CMS-1 | Access Restrictions for Change | Removed; control merged with AC-3.1 |
| CM-6.1 | Configuration Settings | Revised punctuation |
| CM-7.0 | Least Functionality | Replaced bullets for clarity |
| ***ARS V2.0 Category:*** | ***CP – Contingency Planning*** | ***CP – Contingency Planning*** |
| CP-3.0 | Contingency Training | Revised for clarity |
| CP-4.0 | Contingency Plan Testing | Revised 800-53r1 security control name and for punctuation |
| CP-4.1 | Contingency Plan Testing | Revised for 800-53r1 and replaced bullets for clarity |
| CP-4.2 | Contingency Plan Testing | Revised for 800-53r1 |
| CP-4.3 | Contingency Plan Testing | Revised for 800-53r1 |
| CP-5.0 | Contingency Plan Update | Revised for clarity |
| CP-6 | Alternate Storage Sites | Revised 800-53r1 security control name |
| CP-6.1 | Alternate Storage Sites | Removed 100-mile distance control |
| CP-6.3 | Alternate Storage Sites | Control added Moderate to be consistent with CP-7 control |
| CP-7.0 | Alternate Processing Sites | Revised 800-53r1 security control name and added HSPD-20 requirement to provide different Recovery Time Objectives (RTO) for Moderate and High |
| CP-7.1 | Alternate Processing Sites | Removed 100-mile distance control |
| CP-8.0 | Telecommunications Services | Revised for HSPD-20 requirement to provide different Recovery Time Objectives (RTO) for Moderate and High |
| CP-8.4 | Telecommunications Services | Revised for 800-53r1 |

| | | |
|---|---|---|
| CP-9.0 | Information System Backups | Revised 800-53r1 security control name, and revised for clarity and to integrate ARS MP-4.CMS-1 and MP-4.CMS2 controls |
| CP-9.1 | Information System Backups | Revised for 800-53r1 |
| **ARS 1.2 Standard No.** | **ARS 1.2 Standard Name** | **ARS 1.2 Standards Category** |
| CP-10.0 | Information System Recovery and Reconstitution | Punctuation and replaced bullets for clarity |
| ***ARS V2.0 Category:*** | ***IA – Identification and Authentication*** | ***IA – Identification and Authentication*** |
| IA-2.1 | User Identification and Authentication | Revised for 800-53r1; High control changed to Moderate-only control |
| IA-3.0 | Device and Host Identification and Authentication | Revised 800-53r1 security control name |
| IA-4.0 | Identifier Management | Revised timeframe for consistency |
| IA-4.CMS-1 | Identifier Management | Revised punctuation |
| IA-5.0 | Authenticator Management | Revised ARS Appendix A reference for clarity and consistency, and replaced bullets for clarity |
| IA-6.0 | Authenticator Feedback | Revised punctuation |
| IA-7.0 | Cryptographic Module Authentication | Former wording did not deal with authentication to a Cryptographic module - ref FIPS 140-2 section 4.3.3 |
| IA.CMS-1 | Help Desk Support Procedures | Removed; moved to IA-2.CMS-3 |
| ***ARS V2.0 Category:*** | ***IR – Incident Response*** | ***IR – Incident Response*** |
| IR-3.0 | Incident Response Testing | Revised 800-53r1 security control name and revised for 800-53r1 |
| IR-3.1 | Incident Response Testing | Revised for 800-53r1 |
| IR-4.CMS-1 | Incident Handling | Revised to specify proper title |
| ***ARS V2.0 Category:*** | ***MA – Maintenance*** | ***MA – Maintenance*** |
| MA-2.0 | Periodic Maintenance | Revised 800-53r1 security control name and base control removed; included in PISP. Removed Moderate and High add-on controls, and controls included in ARS SI-2 and SI-3.1. |
| MA-2.1 | Periodic Maintenance | Revised for 800-53r1 and removed Low control; revised bullets for clarity |
| MA-2.2 | Periodic Maintenance | Revised for 800-53r1 |
| MA-3.2 | Maintenance Tools | Revised for 800-53r1 |
| MA-3.4 | Maintenance Tools | Revised for 800-53r1 |
| MA-4.1 | Remote Maintenance | Revised for 800-53r1 and added control to Moderate |

| | | |
|---|---|---|
| MA-4.2 | Remote Maintenance | Added control to Moderate |
| MA-4.3 | Remote Maintenance | Revised for 800-53r1 and to include MA-4.0 High add-on control |

| ARS 1.2 Standard No. | ARS 1.2 Standard Name | ARS 1.2 Standards Category |
|---|---|---|
| MA-4.0 | Remote Maintenance | Renumbered as MA-4.CMS-1 and removed MA-4.0 High add-on control which is included in new 800-53r1 MA-4.3 control |
| MA-5.0 | Maintenance Personnel | Revised for consistency |
| MA-CMS-1.CMS-1 | Off-site Physical Repair of Systems | Revised for clarity |
| MA-CMS-2.CMS-1 | On-site Physical Repair of Systems | MA-CMS-2.CMS-2 Moderate and High controls changed to MA-CMS-2.CMS-1 to match Low control |
| MA-CMS-2.CMS-2 | On-site Physical Repair of Systems | MA-CMS-2.CMS-1 Moderate and High controls changed to MA-CMS-2.CMS-2 due to above renumbering |
| ***ARS V2.0 Category:*** | ***MP – Media Protection*** | ***MP – Media Protection*** |
| MP-2.1 | Media Access | Revised for 800-53r1 and added control to Moderate |
| MP-3.0 | Media Labeling | Renumbered and control removed; included in PISP. |
| MP-3.CMS-1 | Media Labeling | Revised for clarity |
| MP-4 | Media Storage | Revised for consistency |
| MP-4.CMS-1 | Media Storage | Removed; control moved to CP-9 |
| MP-4.CMS-2 | Media Storage | Removed; control moved to CP-9 |
| MP-4.CMS-3 | Media Storage | Removed; included in PISP |
| MP-4.CMS-4 | Media Storage | Removed; merged with MP-5.1 |
| MP-5 | Media Transport | Revised for 800-53r1 |
| MP-6.0 | Media Sanitization | Revised 800-53r1 security control name, and revised for clarity and to incorporate MP-7.CMS-1 and MP-7.CMS-2 controls |
| MP-7.CMS-1 | Media Destruction and Disposal | Removed; 800-53r1 control deleted and merged w/MP-6. Former ARS MP-7.CMS-1 controls added to ARS MP-6.0. |
| MP-7.CMS-2 | Media Destruction and Disposal | Removed; 800-53r1 control deleted and merged w/MP-6. Former ARS MP-7.CMS-2 controls added to ARS MP-6.0. |

| | | |
|---|---|---|
| MP-CMS-1 | Media Related Records | Replaced bullets and revised for clarity, and to specify records must allow for reconstruction of the data, if necessary |

| ARS 1.2 Standard No. | ARS 1.2 Standard Name | ARS 1.2 Standards Category |
|---|---|---|
| ***ARS V2.0 Category:*** | ***PE – Physical and Environmental Protection*** | ***PE – Physical and Environmental Protection*** |
| PE-3.CMS-1 | Physical Access Control | Revised for clarity (i.e., data centers include all computing centers not only mainframe centers). |
| PE-3.CMS-2 | Physical Access Control | Renumbered to PE-3.CMS-4 and removed Low control; included in PISP |
| PE-3.CMS-3 | Physical Access Control | Renumbered to PE-3.CMS-2 and revised for clarity |
| PE-3.CMS-4 | Physical Access Control | Renumbered to PE-3.CMS-3 and revised for clarity (i.e., data centers include all computing centers not only mainframe centers). |
| PE-4.CMS-1 | Access Control for Transmission Media | Revised for 800-53r1 and clarity |
| PE-5.0 | Access Control for Display Medium | Renumbered for consistency and removed control; included in PISP |
| PE-6.1 | Monitoring Physical Access | Revised for 800-53r1 |
| PE-6.2 | Monitoring Physical Access | Revised for clarity |
| PE-8.0 | Access Logs | Revised 800-53r1 security control name, and revised control for clarity |
| PE-8.1 | Access Logs | Removed Moderate control |
| PE-10.CMS-1 | Emergency Shutoff | Revised for clarity (i.e., data centers include all computing centers not only mainframe centers). |
| PE-13.1 | Fire Protection | Revised for 800-53r1 |
| PE-13.2 | Fire Protection | Revised for 800-53r1 and control added to Moderate |
| PE-14.CMS-1 | Temperature and Humidity Controls | Revised for clarity |
| PE-15.1 | Water Damage Protection | Revised for clarity |
| PE-17.CMS-1 | Alternate Worksite | Revised 800-53r1 security control name |
| PE-CMS-1.CMS-1 | Power Surge Protection | Removed; control moved to PE-9.CMS-2 |

| | | |
|---|---|---|
| PE-CMS-2.CMS-1 | Physical Ports | Removed; control moved to PE-4.CMS-2 |
| PE-CMS-3.CMS-1 | Restrict the Use of Portable Computing Devices | Removed; control included in AC-19 |
| ***ARS V2.0 Category:*** | ***PL – Planning*** | ***PL – Planning*** |
| PL-2.CMS-1 | System Security Plan | Revised for clarity |
| PL-4.CMS-2 | Rules of Behavior | Revised for clarity |

| ARS 1.2 Standard No. | ARS 1.2 Standard Name | ARS 1.2 Standards Category |
|---|---|---|
| ***ARS V2.0 Category:*** | ***PS – Personnel Security*** | ***PS – Personnel Security*** |
| PS-6.0 | Access Agreements | Revised for 800-53r1 and clarity |
| PS-CMS-1.CMS-1 | Review System Access during Extraordinary Personnel Circumstances | Revised for clarity |
| ***ARS V2.0 Category:*** | ***PS – Personnel Security*** | ***PS – Personnel Security*** |
| RA-3.CMS-1 | Risk Assessments (RA) | Revised 800-53r1 security control name and merged CA-CMS-1.CMS-1 control |
| RA-3.CMS-2 | Risk Assessments (RA) | Removed; control moved to CA-5.CMS-1 |
| RA-4 | Risk Assessments Update | Revised 800-53r1 security control name |
| RA-5.0 | Vulnerability Scanning | Added "Not Required" to Low for consistency |
| RA-5.2 | Vulnerability Scanning | Revised for 800-53r1 |
| ***ARS V2.0 Category:*** | ***SA – System and Services Acquisition*** | ***SA – System and Services Acquisition*** |
| SA-4.CMS-1 | Acquisitions | Revised punctuation |
| SA-8.0 | Security Design Principles | Revised 800-53r1 security control name |
| SA-9.0 | Outsourced Information System Services | Revised 800-53r1 security control name and revised for clarity; renumbered for consistency |
| SA-11 | Developer Security Testing | Revised for punctuation and renumbered for consistency |
| ***ARS V2.0 Category:*** | ***SC – Systems and Communications Protection*** | ***SC – Systems and Communications Protection*** |
| SC-3.2 | Security Function Isolation | Revised for 800-53r1 |
| SC-3.3 | Security Function Isolation | Revised for 800-53r1 |
| SC-3.4 | Security Function Isolation | Revised for 800-53r1 |
| SC-3.5 | Security Function Isolation | Revised for 800-53r1 |
| SC-4.0 | Information Remnants | Revised 800-53r1 security control name |

| | | |
|---|---|---|
| SC-5.0 | Denial-of-Service Protection | Replaced bullets and punctuation for clarity |
| SC-7.CMS-1 | Boundary Protection | Removed; moved to new 800-53r1 SC-7.5 control |
| SC-7.CMS-2 | Boundary Protection | Renumbered to SC-7.CMS-1 |
| SC-7.CMS-3 | Boundary Protection | Renumbered to SC-7.CMS-2 |
| SC-7.CMS-4 | Boundary Protection | Renumbered to SC-7.CMS-3 |
| SC-7.1 | Boundary Protection | Revised for clarity and consistency |
| SC-7.CMS-1 | Boundary Protection | New 800-53r1 enhancement; renumbered and moved former SC-7.CMS-1 control here |
| **ARS 1.2 Standard No.** | **ARS 1.2 Standard Name** | **ARS 1.2 Standards Category** |
| SC-8.CMS-1 | Transmission Integrity | Revised; encryption for confidentiality is addressed in SC-9.CMS-1. |
| SC-8.1 | Transmission Integrity | Revised for clarity and control added to Moderate for consistency (i.e., SC-8.CMS-1 is Moderate) |
| SC-9.CMS-1 | Transmission Confidentiality | Removed; replaced by revised SC-9.1 |
| SC-9.1 | Transmission Confidentiality | Revised for 800-53r1 and for clarity; control added to Moderate for consistency (i.e.,SC-9.CMS-1 is Moderate) |
| SC-10.0 | Network Disconnect | Revised punctuation |
| SC-10.CMS-1 | Network Disconnect | Removed; included in AC-11 |
| SC-10.CMS-2 | Network Disconnect | Removed; included in AC-11 |
| SC-11 | Trusted Path | Revised for 800-53r1 and renumbered to SC-11.0 for consistency |
| SC-12.CMS-1 | Cryptographic Key Management | Revised 800-53r1 security control name and revised for consistency |
| SC-13 | Use of Cryptography | Revised 800-53r1 security control name |
| SC-14.CMS-2 | Public Access Protections | Revised ARS Appendix A reference for clarity and consistency |
| SC-15.CMS-1 | Collaborative Computing | Revised for 800-53r1 and punctuation |
| SC-19.CMS-1 | Voice Over Internet Protocol | Changed acronym and revised for clarity |
| SC-CMS-2.CMS-1 | Identify and Detect Unauthorized Modems | Revised for clarity and punctuation |
| SC-CMS-3.CMS-1 | Secondary Authentication and Encryption | Revised punctuation and revised security mechanism |

| | | |
|---|---|---|
| SC-CMS-3.CMS-2 | Secondary Authentication and Encryption | Revised ARS Appendix A reference for clarity and consistency |
| SC-CMS-4.CMS-1 | Electronic Mail | Revised for clarity |
| SC-CMS-5.CMS-1 | Persistent Cookies | Revised for clarity |
| ***ARS V2.0 Category:*** | ***SI – System and Information Integrity*** | ***SI – System and Information Integrity*** |
| SI-2.0 | Flaw Remediation | Replaced bullets for clarity |
| SI-2.1 | Flaw Remediation | Revised for 800-53r1 and clarity |
| SI-2.2 | Flaw Remediation | Revised for 800-53r1 |
| SI-3.CMS-1 | Malicious Code Protection | Revised for 800-53r1 |
| SI-3.1 | Malicious Code Protection | Revised for 800-53r1 |
| SI-3.2 | Malicious Code Protection | Revised for 800-53r1 |
| **ARS 1.2 Standard No.** | **ARS 1.2 Standard Name** | **ARS 1.2 Standards Category** |
| SI-4.CMS-1 | Intrusion Detection Tools and Techniques | Revised 800-53r1 security control name |
| SI-4.CMS-2 | Intrusion Detection Tools and Techniques | Removed; replaced by new 800-53r1 SI-4.5 control |
| SI-4.2 | Intrusion Detection Tools and Techniques | Revised for 800-53r1 |
| SI-4.4 | Intrusion Detection Tools and Techniques | Revised for 800-53r1 and added control Moderate |
| SI-5.1 | Security Alerts and Advisories | Revised for clarity |
| SI-6.1 | Security Functionality Verification | Revised for 800-53r1 |
| SI-8 | Spam and Spyware Protection | Revised 800-53r1 security control name |
| SI-8.1 | Spam and Spyware Protection | Revised for 800-53r1 |
| SI-8.2 | Spam and Spyware Protection | Revised for 800-53r1 |
| SI-10.CMS-1 | Information Input Accuracy, Completeness, and Validity | Revised 800-53r1 security control name and control for 800-53r1 |
| SI-12.1 | Information Output Handling and Retention | Revised for 800-53r1 and renumbered to SI-12.0 for consistency |