Memorandum for Record: Security Controls Assessment Form

In the FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, OMB stated that for fiscal year (FY) 2007 and beyond, "agencies will be required to use FIPS 200/NIST Special Publication 800-53 for the specification of security controls and NIST Special Publication 800-53A for the assessment of security control effectiveness."

After the final release of SP 800-53A in FY 2007, NIST plans to rescind SP 800-26, *Security Self Assessment Guide for Information Technology Systems*. The security controls assessment form, accessible at http://csrc.nist.gov/ (under CSD News), intends to replace the assessment form contained in SP 800-26 and provide a standard methodology for capturing the results of system-level security controls assessments by providing a form to comprehensively, consistently, and cost-effectively show the results of a security controls assessment. This form will be incorporated into the final release of SP 800-53A.

Agencies may use the attached instructions and form to support security controls assessment requirements for FY 2007. If agencies wish to use the annual assessment for system recertification purposes for High or Moderate impact systems, an independent assessment of a security control's effectiveness must be performed.

Attachment: Security Controls Assessment Guideline and Form

Security control assessments provide a line of defense in knowing the strengths and weaknesses of an organization's information system. Security controls assessment determines whether security controls in an information system are operating as intended. The results of this assessment are used in determining the overall effectiveness of the security controls in an information system, identifying residual vulnerabilities in the system, providing credible and meaningful inputs to the organization's Plan of Action and Milestones (POA&M), and supporting the Authorizing Official's accreditation decision. A well executed security controls assessment validates the security controls contained in the information system security plan and facilitates a cost-effective approach to correcting deficiencies in the system in an orderly and disciplined manner consistent with the organization's mission requirements.

This document is intended to help standardize the security controls assessment results to aid agencies in clearly and cost-effectively:

- Assessing information systems annually as required by FISMA, through the continuous monitoring security control process;
- Preparing for program and system audits and reviews;
- Performing assessment activities in support of Certification & Accreditation; and
- Providing possible metrics of the information security posture of an agency.

Selection of Security Controls to Assess

All security controls applicable to an information system must be assessed prior to the initial accreditation and at least once during each subsequent three-year system reaccreditation period. Realizing that it is neither feasible nor cost-effective to monitor all of the security controls in any information system on a continuous basis, it is recommended that the organization establish a schedule for security control monitoring to ensure that all controls requiring more frequent monitoring are adequately covered and that all controls are covered at least once between each accreditation decision.

Organizations have flexibility in determining which, and how many, controls are assessed on an annual basis, provided all security controls applicable to the information system are assessed over the course of the system accreditation period[1].

There are many factors that may influence and, in some cases, drive the selection of a subset of security controls to assess, including:

- *Annual Security Control Requirements* – NIST SP 800-53 identifies several security controls that require execution at least annually. Those security controls that require at least annual execution are good candidates for annual assessment. Examples of security controls included in NIST SP 800-53 that require execution

1 In support of the security certification process, NIST SP 800-53 Revision 1, Security Control *CA-4: Security Certification* requires an independent assessment of security controls for those systems with a FIPS 199 impact rating of Moderate or High.

at least annually include, but may not be limited to, AC-2, AT-2, CA-2, CP-3, CP-4, CP-5, IR-2, IR-3, PE-2, and PL-3. An organization may define additional security controls that require annual execution based on the results of a risk assessment, or as required by organizational policy.

Agencies may also take credit for assessing the effectiveness of those annually executed security controls provided they document the following in the security controls assessment form:

- Evidence that the security control was executed annually; and
- Any findings identified as a result of the security control execution.

- *Significant changes to the information system* – A significant change to an information system, or its operating environment, may introduce new security vulnerabilities and considerations, and may require a more frequent assessment of some or all security controls[2].

- *External influences* – Activities outside the direct control of the information system frequently impact the security posture, and control selection, of the information system. Examples may include, but are not limited to, organizational changes, new or modified policies, and newly identified threats or vulnerabilities. These external influences may affect the risk profile of the system, possibly resulting in the need to assess some security controls more frequently or sooner than otherwise planned.

- *Organizational requirements and priorities* – Those security controls that the organization deems essential to protecting the information system may require increased attention, and more frequent assessment. Additionally, organizations may want to assess progress towards a specific information security goal such as an Agency campaign targeted at improving security awareness among its users.

- *POA&M items* – New or modified security controls, implemented to remediate identified weaknesses, should be assessed for effectiveness.

These factors may impact the subset of security controls selected for assessment, as well as the frequency that certain security controls are assessed. To ensure greater alignment with organizational and risk-based priorities, the security controls assessment should be planned and conducted in close coordination with the authorizing official and the senior agency information security officer.

2 Examples of significant changes may include, but are not limited, to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, may also play a role in security controls selected for assessment.

Documenting the Results of the Security Controls Assessment

The Security Controls Assessment form can be used to document the assessment results for each security control. This template, once completed, may be used to identify the status of security controls for a system or an interconnected group of systems. Assessing all security controls and all interconnected system dependencies, documenting in a standardized format, and analyzing the results provide one possible metric of the information security posture of an agency. Until the final release of NIST SP 800-53A, the assessment procedures detailed in draft NIST SP 800-53A[3] should be used for each applicable security control.

The Security Controls Assessment form contains two sections: the System Overview and the Form Table. The first section, the System Overview, is taken primarily from the System Security Plan (SSP) and requires basic descriptive information about the information system being assessed, as well as the assessment environment.

Section two, the Form Table, includes the seventeen control families contained in NIST SP 800-53 and the security controls and enhancements within each family, as well as those fields necessary to capture the assessment environment and results. The form should be modified to show only the security controls identified in the SSP for the information system. This modified form can then be provided to the information system owner, the information system security officer, and/or the independent assessor who is evaluating the system or systems.

The Security Controls Assessment form may be further customized by the organization prior to being used in the assessment process. An organization can require more descriptive information and pre-populate assessment results for certain security controls if applicable. For example, many agencies may have common controls (e.g., personnel security procedures, physical security procedures, awareness and training) that apply to all systems within the agency. The status as a common control, with associated information on the organizational element responsible for the control, may be pre-populated. Additional columns may be added to reflect the status of the control (e.g., planned action date, location of documentation).

An agency may also have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. If specific agency requirements necessitate additional security controls, those security controls should be documented in the system security plan and added to this system-level assessment form.

---

3 OMB M-06-20, *FY2006 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management*, stated that, for FY07 and beyond, "agencies will be required to use FIPS 200/NIST Special Publication 800-53 for the specification of security controls and NIST Special Publication 800-53A for the assessment of security control effectiveness."

Data Element Descriptions

The remainder of this document provides a detailed description of each data element on the security controls assessment form. Agencies should have an established policy on how the security controls assessments are to be controlled and how assessment information is accessed prior to initiation of the activity.

System Overview Data Elements

The following data elements are captured in the System Overview:

1. System Name and Identifier –

The first item listed in the security controls assessment form is the system name and identifier which should be copied from the SSP.

2. Security Categorization –

In this section, copy from the SSP the FIPS 199 impact level (High, Moderate, Low) for each security objective (confidentiality, integrity, availability), as well as the overall system categorization level, which is based on the high watermark of the underlying security objectives impact levels.

3. General System Description/Purpose –

This field is optional. The General System Description/Purpose found in the SSP may be summarized and inserted into this section of the assessment form.

4. List of Connected Systems –

This field is optional. A list of connected systems found in the SSP may be included in this section. For each connected system, also provide the FIPS 199 category and the accreditation date.

Form Table Data Elements

The following data elements are captured in the Form Table

1. Security Control Number –

The Security Control Number is defined in NIST SP 800-53.

2. Security Control Name –

The Security Control Name is defined in NIST SP 800-53.

3. Security Control and Enhancements –

The Security Controls and Enhancements are defined in NIST SP 800-53. In this form table, all security controls and enhancements from NIST SP 800-53 are provided. Agencies should modify this table prior to assessment to reflect those security controls found in the SSP.

4. Baseline Applicability –

The Baseline Applicability for each security control and enhancement can be found in NIST SP 800-53.

5. Security Control Type –

The security control type identifies the security control scope within the organization. This data element is as defined in the SSP. Refer to Table 1 below for a description of each security control type, as well as expectations for assessment and reporting.

Table 1: Security Control Types

Security Control Type	Description	Assessment and Reporting Expectations
Common	A security control that can be applied to one or more organizational information systems, and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.	Use the *Assessment Evidence* field in the *Security Controls Assessment Reporting Template* to identify who is responsible for the common security control implementation. This information can be transcribed from the SSP. The party responsible for the common security control implementation is also responsible for assessing the effectiveness of the security control. As a matter of due diligence, each information system owner benefiting from a common security control is responsible for verifying its assessed effectiveness.
System-Specific	A security control for an information system that has not been designed as a common control, and is the responsibility of the information system owner.	Each information system owner is responsible for ensuring all security controls for which they are responsible are assessed, and the results of the assessment adequately documented in the Security Controls Assessment Reporting Template.
Hybrid	As defined in the SSP, the organization may assign a *hybrid* status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific.	For the Common security control portion, an information system owner should follow the assessment and reporting expectations for a common security control. For the System-Specific security control component, an information system owner should follow the assessment and reporting expectations for a system-specific security control.

6. Last Date Security Control Assessed –

Provide the most recent date each applicable control has been assessed. All applicable controls that have been implemented must be assessed at least once during the system accreditation period. A subset of agency-selected controls must be assessed annually, including those specific controls that require annual assessment.

7. Assessor Information–

In this field, record (1) the name of the security control assessor, and (2) the assessor's degree of independence. Response options for the assessor's degree of independence are "self" and "independent". An assessor capable of conducting an impartial assessment is considered "independent". All other assessors are considered "self". For FIPS 199 Moderate and High impact systems, all security controls must be assessed independently at least once during the accreditation period.

The assessor independence identifies the degree to which the assessor is capable of conducting an impartial assessment of an information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness.

An independent assessment of a security control's effectiveness must be performed for FIPS 199 Moderate and High impact systems when the assessment is supporting the system security certification.

Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment of the security controls be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

It is expected that this form will be used throughout a three year system security accreditation period. If desired, agencies may have different assessors at different times for different controls.

8. Assessed Security Control Effectiveness –

Applying the assessment methods and associated procedural statements designated in draft NIST SP 800-53A produces results that are used to determine whether a particular security control is operating as intended (i.e., is the control implemented correctly, being used as intended, and producing the intended outcome with respect to meeting the security requirements for the information system).

Response options include *Satisfied*, *Partially Satisfied*, and *Not Satisfied*. *Satisfied* indicates that the portion(s) of the security control being addressed by the procedural statement are operating as intended. *Partially Satisfied* indicates that some portion(s) of the security control being addressed by the procedural statement are operating as intended, but other portions being addressed are not. *Not Satisfied* indicates that the portion(s) of the security control being addressed by the procedural statement are not operating as intended. Remediation plans for those security controls whose effectiveness is assessed as partially or not satisfied should be captured in the organization's POA&M.

Documented evidence and results supporting the assessed security control effectiveness should be recorded in the Assessment Evidence field of this template.

9. Assessment Steps Used –

Assessment Steps are those procedural statements executed to assess a particular aspect of a security control. Appendix F in draft NIST SP 800-53A provides a catalog of assessment procedures for the security controls and enhancements in NIST SP 800-53.

In this field, assessors should identify those assessment procedures from draft NIST SP 800-53A used to determine the assessed security control effectiveness.

10. Assessment Evidence –

During the assessment process, assessors should gather as much evidence as needed to support the assessed level of security control effectiveness.

In this field, include a description and/or references to information obtained during the assessment process that supports the assessed level of security control effectiveness. Examples of assessment evidence that agencies may wish to record in this field include, but are not limited to, references to relevant policies, procedures, plans, and other documentation examined during the security control assessment; a listing of personnel interviewed during the assessment of the security control, a short description of the information obtained from interviews conducted; a description of functional tests performed, and the results of the functional tests or a reference to where the results are available.

If a security control is assessed and determined to be either *partially satisfied* or *not satisfied*, the assessor should also indicate which portions of the security control are operating as intended, and which portions are not operating as intended.

Security Controls Assessment Form

System Overview

System Name and Identifier	
Security Categorization: FIPS 199 Impact Level	
System (based on high water mark of security objectives impact level)	High ☐ Moderate ☐ Low ☐
Confidentiality (based on high water mark of information type impact levels)	High ☐ Moderate ☐ Low ☐
Integrity (based on high water mark of information type impact levels)	High ☐ Moderate ☐ Low ☐
Availability (based on high water mark of information type impact levels)	High ☐ Moderate ☐ Low ☐
General System Description/Purpose	
List of Connected Systems	

System Name	**FIPS 199 Category**	**Accreditation Date**

Table: Security Controls Assessment

Security Control Family: Access Control (AC)

Sec Ctrl #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AC-1	Access Control Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	X	X	X						
AC-2	Account Management	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment*: organization-defined frequency, at least annually].	X	X	X						
AC-2.1		The organization employs automated mechanisms to support the management of information system accounts.		X	X						
AC-2.2		The information system automatically terminates temporary and emergency accounts after [*Assignment*: organization-defined time period for		X	X						

Sec Ctrl #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		each type of account].									
AC-2.3		The information system automatically disables inactive accounts after [*Assignment*: organization-defined time period].		X	X						
AC-2.4		The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.		X	X						
AC-3	Access Enforcement	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	X	X	X						
AC-3.1		The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).		X	X						
AC-4	Information Flow Enforcement	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		X	X						
AC-4.1		The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.									

Sec Ctrl #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AC-4.2		The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.									
AC-4.3		The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.									
AC-5	Separation of Duties	The information system enforces separation of duties through assigned access authorizations.		X	X						
AC-6	Least Privilege	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.		X	X						
AC-7	Unsuccessful Login Attempts	The information system enforces a limit of [*Assignment*: organization-defined number] consecutive invalid access attempts by a user during a [*Assignment*: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [*Assignment*: organization-defined time period], delays next login prompt according to *Assignment*: organization-defined delay algorithm.] when the maximum number of unsuccessful attempts is exceeded.	X	X	X						

Sec Ctrl #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AC-7.1		The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.									
AC-8	System Use Notification	The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.	X	X	X						
AC-9	Previous Logon Notification	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.									
AC-10	Concurrent Session Control	The information system limits the number of concurrent sessions for any user to [*Assignment*: organization-defined number of sessions].			X						

Sec Ctrl #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AC-11	Session Lock	The information system prevents further access to the system by initiating a session lock after [*Assignment*: organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.		X	X						
AC-12	Session Termination	The information system automatically terminates a session after [*Assignment*: organization-defined time period] of inactivity.		X	X						
AC-12.1		Automatic session termination applies to local and remote sessions.			X						
AC-13	Supervision and Review - Access Control	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.	X	X	X						
AC-13.1		The organization employs automated mechanisms to facilitate the review of user activities.		X	X						
AC-14	Permitted Actions without Identification or Authentication	The organization identifies specific user actions that can be performed on the information system without identification or authentication.	X	X	X						

Sec Ctrl #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AC-14.1		The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.		X	X						
AC-15	Automated Marking	The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.			X						
AC-16	Automated Labeling	The information system appropriately labels information in storage, in process, and in transmission.									
AC-17	Remote Access	The organization authorizes, monitors, and controls all methods of remote access to the information system.	X	X	X						
AC-17.1		The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.		X	X						
AC-17.2		The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.		X	X						
AC-17.3		The organization controls all remote accesses through a managed access control points.		X	X						
AC-17.4		The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the		X	X						

Sec Ctrl #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		information system.									
AC-18	Wireless Access Restrictions	The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.	X	X	X						
AC-18.1		The organization uses authentication and encryption to protect wireless access to the information system.		X	X						
AC-18.2		The organization scans for unauthorized wireless access points [*Assignment*: organization-defined frequency] and takes appropriate action if such an access points are discovered.			X						
AC-19	Access Control for Portable and Mobile Devices	The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.		X	X						
AC-20	Use of External Information Systems	The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an	X	X	X						

Sec Ctrl #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		external information system.									
AC-20.1		The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify		X	X						

Security Control Family: Awareness and Training (AT)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AT-1	Security Awareness and Training Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	X	X	X						
AT-2	Security Awareness	The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*Assignment*: organization-defined frequency, at least annually] thereafter.	X	X	X						
AT-3	Security Training	The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment*: organization-defined	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		frequency] thereafter.									
AT-4	Security Training Records	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.	X	X	X						
AT-5	Contacts with Security Groups and Associations	The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.									

Security Control Family: Audit and Accountability (AU)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AU-1	Audit and Accountability Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	X	X	X						
AU-2	Auditable Events	The information system generates audit records for the following events: [*Assignment*: organization-defined auditable events].	X	X	X						
AU-2.1		The information system provides the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail.			X						
AU-2.2		The information system provides the capability to manage the selection of events to be audited by individual components of the system.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AU-2.3		The organization periodically reviews and updates the list of organization-defined auditable events.		X	X						
AU-3	Content of Audit Records	The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.	X	X	X						
AU-3.1		The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.		X	X						
AU-3.2		The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.			X						
AU-4	Audit Storage Capacity	The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	X	X	X						
AU-5	Response to Audit Processing Failures	The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [*Assignment*: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AU-5.1		The information system provides a warning when allocated audit record storage volume reaches [*Assignment*: organization-defined percentage of maximum audit record storage capacity].			X						
AU-5.2		The information system provides a real-time alert when the following audit failure events occur: [*Assignment*: organization-defined audit failure events requiring real-time alerts].			X						
AU-6	Audit Monitoring, Analysis, and Reporting	The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.		X	X						
AU-6.1		The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.			X						
AU-6.2		The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment*: organization-defined list of inappropriate or unusual activities that are to result in		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
AU-7	Audit Reduction and Report Generation	The information system provides an audit reduction and report generation capability.		X	X						
AU-7.1		The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.		X	X						
AU-8	Time Stamps	The information system provides time stamps for use in audit record generation.	X	X	X						
AU-8.1		The organization synchronizes internal information system clocks [*Assignment*: organization-defined frequency].		X	X						
AU-9	Protection of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	X	X	X						
AU-9.1		The information system produces audit records on hardware-enforced, write-once media.									
AU-10	Non-Repudiation	The information system provides the capability to determine whether a given individual took a particular action.									
AU-11	Audit Record Retention	The organization retains audit records for [*Assignment*: organization-defined time period] to provide support for after-the-fact investigations of security	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		incidents and to meet regulatory and organizational information retention requirements.									

Security Control Family: Certification, Accreditation, and Security Assessments (CA)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.	X	X	X						
CA-2	Security Assessments	The organization conducts an assessment of the security controls in the information system [*Assignment*: organization-defined frequency, at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	X	X	X						
CA-3	Information System Connections	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		basis.									
CA-4	Security Certification	The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	X	X	X						
CA-4.1		The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.		X	X						
CA-5	Plan of Actions and Milestones	The organization develops and updates [*Assignment*: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	X	X	X						
CA-6	Security Accreditation	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment*: organization-defined frequency, at least every three years] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CA-7	Continuous Monitoring	The organization monitors the security controls in the information system on an ongoing basis.	X	X	X						
CA-7.1		The organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.									

Security Control Family: Configuration Management (CM)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CM-1	Configuration Management Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	X	X	X						
CM-2	Baseline Configuration	The organization develops, documents, and maintains a current baseline configuration of the information system.	X	X	X						
CM-2.1		The organization updates the baseline configuration of the information system as an integral part of information system component installations.		X	X						
CM-2.2		The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CM-3	Configuration Change Control	The organization authorizes, documents, and controls changes to the information system		X	X						
CM-3.1		The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.			X						
CM-4	Monitoring Configuration Change	The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.		X	X						
CM-5	Access Restrictions for Change	The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.		X	X						
CM-5.1		The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.			X						
CM-6	Configuration Settings	The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.									
CM-6.1		The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.			X						
CM-7	Least Functionality	The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment*: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].		X	X						
CM-7.1		The organization reviews the information system [*Assignment*: organization-defined frequency], to identify and eliminate unnecessary functions, ports, protocols, and/or services.			X						
CM-8	Information System Component Inventory	The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.	X	X	X						
CM-8.1		The organization updates the inventory of information system components as an integral part of component		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		installations.									
CM-8.2		The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.			X						

Security Control Family: Contingency Planning (CP)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CP-1	Contingency Planning Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	X	X	X						
CP-2	Contingency Plan	The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.	X	X	X						
CP-2.1		The organization coordinates contingency plan development with organizational elements responsible for related plans.		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CP-2.2		The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.			X						
CP-3	Contingency Training	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment*: organization-defined frequency, at least annually].		X	X						
CP-3.1		The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.			X						
CP-3.2		The organization employs automated mechanisms to provide a more thorough and realistic training environment.									
CP-4	Contingency Plan Testing and Exercises	The organization: (i) tests and/or exercises the contingency plan for the information system [*Assignment*: organization-defined frequency, at least annually] using [*Assignment*: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CP-4.1		The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.		X	X						
CP-4.2		The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.			X						
CP-4.3		The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan 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	Contingency Plan Update	The organization reviews the contingency plan for the information system [*Assignment*: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	X	X	X						
CP-6	Alternate Storage Site	The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CP-6.1		The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.		X	X						
CP-6.2		The organization configures the alternate storage site to facilitate timely and effective recovery operations.			X						
CP-6.3		The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		X	X						
CP-7	Alternate Processing Site	The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*Assignment*: organization-defined time period] when the primary processing capabilities are unavailable.		X	X						
CP-7.1		The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.		X	X						
CP-7.2		The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CP-7.3		The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.		X	X						
CP-7.4		The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.			X						
CP-8	Telecommunications Services	The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*Assignment*: organization-defined time period] when the primary telecommunications capabilities are unavailable.		X	X						
CP-8.1		The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.		X	X						
CP-8.2		The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CP-8.3		The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.			X						
CP-8.4		The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.			X						
CP-9	Information System Backup	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment*: organization-defined frequency] and protects backup information at the storage location.	X	X	X						
CP-9.1		The organization tests backup information [*Assignment*: organization-defined frequency] to ensure media reliability and information integrity.		X	X						
CP-9.2		The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.			X						
CP-9.3		The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
CP-9.4		The organization protects system backup information from unauthorized modification.		X	X						
CP-10	Information System Recovery and Reconstitution	The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.	X	X	X						
CP-10.1		The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.			X						

Security Control Family: Identification and Authentication (IA)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
IA-1	Identification and Authentication Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	X	X	X						
IA-2	User Identification and Authentication	The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	X	X	X						
IA-2.1		(1) The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 [Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4] compliant.		X							
IA-2.2		The information system employs multifactor authentication for local system access that is NIST Special Publication 800-63 [Selection: organization-defined level 3 or level 4]			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		compliant.									
IA-2.3		The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 level 4 compliant.			X						
IA-3	Device Identification and Authentication	The information system identifies and authenticates specific devices before establishing a connection.		X	X						
IA-4	Identifier Management	The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [*Assignment*: organization-defined time period] of inactivity; and (vi) archiving user identifiers.	X	X	X						
IA-5	Authenticator Management	The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
IA-6	Authenticator Feedback	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	X	X	X						
IA-7	Cryptographic Module Authentication	The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	X	X	X						

Security Control Family: Incident Response (IR)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
IR-1	Incident Response Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	X	X	X						
IR-2	Incident Response Training	The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment*: organization-defined frequency, at least annually].		X	X						
IR-2.1		The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.			X						
IR-2.2		The organization employs automated mechanisms to provide a more thorough and realistic training environment.									

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
IR-3	Incident Response Testing and Exercises	The organization tests and/or exercises the incident response capability for the information system [*Assignment*: organization-defined frequency, at least annually] using [*Assignment*: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.		X	X						
IR-3.1		The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.			X						
IR-4	Incident Handling	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	X	X	X						
IR-4.1		The organization employs automated mechanisms to support the incident handling process.		X	X						
IR-5	Incident Monitoring	The organization tracks and documents information system security incidents on an ongoing basis.		X	X						
IR-5.1		The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
IR-6	Incident Reporting	The organization promptly reports incident information to appropriate authorities.	X	X	X						
IR-6.1		The organization employs automated mechanisms to assist in the reporting of security incidents.		X	X						
IR-7	Incident Response Assistance	The organization provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.	X	X	X						
IR-7.1		The organization employs automated mechanisms to increase the availability of incident response-related information and support.		X	X						

Security Control Family: Maintenance (MA)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
MA-1	System Maintenance Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	X	X	X						
MA-2	Periodic Maintenance	The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.	X	X	X						
MA-2.1		The organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance		X	X						
MA-2.2		The organization employs automated mechanisms to schedule and conduct			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		maintenance as required, and to create up-to date, accurate, complete, and available records of all maintenance actions, both needed and completed.									
MA-3	Maintenance Tools	The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.		X	X						
MA-3.1		The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.			X						
MA-3.2		The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.			X						
MA-3.3		The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
MA-3.4		The organization employs automated mechanisms to ensure only authorized personnel use maintenance tools.									
MA-4	Remote Maintenance	The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.	X	X	X						
MA-4.1		The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions		X	X						
MA-4.2		The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.		X	X						
MA-4.3		The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless t			X						
MA-5	Maintenance Personnel	The organization allows only authorized personnel to perform maintenance on the information system.	X	X	X						
MA-6	Timely Maintenance	The organization obtains maintenance support and spare parts for [*Assignment*: organization-defined list of key information system		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		components] within [*Assignment*: organization-defined time period] of failure.									

Security Control Family: Media Protection (MP)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
MP-1	Media Protection Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	X	X	X						
MP-2	Media Access	The organization restricts access to information system media to authorized individuals.	X	X	X						
MP-2.1		The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.		X	X						
MP-3	Media Labeling	The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts [*Assignment*: organization-defined list of media types or hardware components] from labeling so long as they remain within [*Assignment*: organization-defined protected			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		environment].									
MP-4	Media Storage	The organization physically controls and securely stores information system media within controlled areas.		X	X						
MP-5	Media Transport	The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.		X	X						
MP-5.1		The organization protects digital and non-digital media during transport outside of controlled areas using [*Assignment*: organization-defined security measures, e.g., locked container, cryptography].		X	X						
MP-5.2		The organization documents, where appropriate, activities associated with the transport of information system media using [*Assignment*: organization-defined system of records].		X	X						
MP-5.3		The organization employs an identified custodian at all times to transport information system media.			X						
MP-6	Media Sanitization and Disposal	The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
MP-6.1		The organization tracks, documents, and verifies media sanitization and disposal actions.			X						
MP-6.2		The organization periodically tests sanitization equipment and procedures to verify correct performance.			X						

Security Control Family: Physical and Environmental Protection (PE)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
PE-1	Physical and Environmental Protection Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	X	X	X						
PE-2	Physical Access Authorizations	The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [*Assignment*: organization-defined frequency, at least annually].	X	X	X						
PE-3	Physical Access Control	The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.									
PE-3.1		The organization controls physical access to the information system independent of the physical access controls for the facility.			X						
PE-4	Access Control for Transmission Medium	The organization controls physical access to information system distribution and transmission lines within organizational facilities.			X						
PE-5	Access Control for Display Medium	The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.		X	X						
PE-6	Monitoring Physical Access	The organization monitors physical access to information systems to detect and respond to incidents.	X	X	X						
PE-6.1		The organization monitors real-time intrusion alarms and surveillance equipment.		X	X						
PE-6.2		The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		response actions.									
PE-7	Visitor Control	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	X	X	X						
PE-7.1		The organization escorts visitors and monitors visitor activity, when required.		X	X						
PE-8	Access Records	The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [*Assignment*: organization-defined frequency].	X	X	X						
PE-8.1		The organization employs automated mechanisms to facilitate the maintenance and review of access logs.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
PE-8.2		The organization maintains a record of all physical access, both visitor and authorized individuals.			X						
PE-9	Power Equipment and Power Cabling	The organization protects power equipment and power cabling for the information system from damage and destruction.		X	X						
PE-9.1		The organization employs redundant and parallel power cabling paths.									
PE-10	Emergency Shutoff	The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.		X	X						
PE-10.1		The organization protects the emergency power-off capability from accidental or unauthorized activation.			X						
PE-11	Emergency Power	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.		X	X						
PE-11.1		The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		operational capability in the event of an extended loss of the primary power source.									
PE-11.2		The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.									
PE-12	Emergency Lighting	The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.	X	X	X						
PE-13	Fire Protection	The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.	X	X	X						
PE-13.1		The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.		X	X						
PE-13.2		The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.		X	X						
PE-13.3		The organization employs an automatic fire suppression capability in facilities that are not staffed on a		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		continuous basis.									
PE-14	Temperature and Humidity Controls	The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.	X	X	X						
PE-15	Water Damage Protection	The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	X	X	X						
PE-15.1		The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.			X						
PE-16	Delivery and Removal	The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.	X	X	X						
PE-17	Alternate Work Site	The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
PE-18	Location of Information System Components	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.		X	X						
PE-18.1		The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.			X						
PE-19	Information Leakage	The organization protects the information system from information leakage due to electromagnetic signals emanations.									

Security Control Family: Planning (PL)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
PL-1	Security Planning Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	X	X	X						
PL-2	System Security Plan	The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	X	X	X						
PL-3	System Security Plan Update	The organization reviews the security plan for the information system [*Assignment*: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
PL-4	Rules of Behavior	The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.	X	X	X						
PL-5	Privacy Impact Assessment	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	X	X	X						
PL-6	Security-Related Activity Planning	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.		X	X						

Security Control Family: Personnel Security (PS)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
PS-1	Personnel Security Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	X	X	X						
PS-2	Position Categorization	The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [*Assignment: organization-defined frequency*].	X	X	X						
PS-3	Personnel Screening	The organization screens individuals requiring access to organizational information and information systems before authorizing access.	X	X	X						
PS-4	Personnel Termination	The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		official records created by the terminated employee that are stored on organizational information systems.									
PS-5	Personnel Transfer	The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.	X	X	X						
PS-6	Access Agreements	The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [*Assignment: organization-defined frequency*].	X	X	X						
PS-7	Third-Party Personnel Security	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.	X	X	X						
PS-8	Personnel Sanctions	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	X	X	X						

Security Control Family: Risk Assessment (RA)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
RA-1	Risk Assessment Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	X	X	X						
RA-2	Security Categorization	The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.	X	X	X						
RA-3	Risk Assessment	The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).									
RA-4	Risk Assessment Update	The organization updates the risk assessment [*Assignment*: organization-defined frequency] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.	X	X	X						
RA-5	Vulnerability Scanning	The organization scans for vulnerabilities in the information system [*Assignment*: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.		X	X						
RA-5.1		The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.			X						
RA-5.2		The organization updates the list of information system vulnerabilities scanned [*Assignment*: organization-defined frequency] or when significant new vulnerabilities are identified and reported.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
RA-5.3		The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.									

Security Control Family: System and Services Acquisition (SA)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SA-1	System and Services Acquisition Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	X	X	X						
SA-2	Allocation of Resources	The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.	X	X	X						
SA-3	Life Cycle Support	The organization manages the information system using a system development life cycle methodology that includes information security considerations.	X	X	X						
SA-4	Acquisitions	The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.									
SA-4.1		The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.		X	X						
SA-4.2		The organization requires in solicitation documents that appropriate documentation be provided describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).									
SA-5	Information System Documentation	The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	X	X	X						
SA-5.1		The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		detail to permit analysis and testing of the controls.									
SA-5.2		The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).			X						
SA-6	Software Usage Restrictions	The organization complies with software usage restrictions.	X	X	X						
SA-7	User Installed Software	The organization enforces explicit rules governing the downloading and installation of software by users.	X	X	X						
SA-8	Security Engineering Principles	The organization designs and implements the information system using security engineering principles.		X	X						
SA-9	External Information System Services	The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SA-10	Developer Configuration Management	The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.			X						
SA-11	Developer Security Testing	The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.		X	X						

Security Control Family: System and Communications Protection (SC)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SC-1	System and Communications Protection Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	X	X	X						
SC-2	Application Partitioning	The information system separates user functionality (including user interface services) from information system management functionality.		X	X						
SC-3	Security Function Isolation	The information system isolates security functions from non-security functions.			X						
SC-3.1		The information system employs underlying hardware separation mechanisms to facilitate security function isolation.									
SC-3.2		The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both									

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		non-security functions and from other security functions.									
SC-3.3		The information system minimizes the number of non-security functions included within the isolation boundary containing security functions.									
SC-3.4		The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.									
SC-3.5		The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.									
SC-4	Information Remnance	The information system prevents unauthorized and unintended information transfer via shared system resources.		X	X						
SC-5	Denial of Service Protection	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment*: organization-defined list of types of denial of service attacks or reference to source for current list].		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SC-5.1		The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.									
SC-5.2		The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.									
SC-6	Resource Priority	The information system limits the use of resources by priority.									
SC-7	Boundary Protection	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	X	X	X						
SC-7.1		The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.		X	X						
SC-7.2		The organization prevents public access into the organization's internal networks except as appropriately mediated.		X	X						
SC-7.3		The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SC-7.4		The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.		X	X						
SC-7.5		The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).		X	X						
		The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.			X						
SC-8	Transmission Integrity	The information system protects the integrity of transmitted information.		X	X						
SC-8.1		The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SC-9	Transmission Confidentiality	The information system protects the confidentiality of transmitted information.		X	X						
SC-9.1		The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.			X						
SC-10	Network Disconnect	The information system terminates a network connection at the end of a session or after [*Assignment*: organization-defined time period] of inactivity.		X	X						
SC-11	Trusted Path	The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment*: organization-defined security functions to include at a minimum, information system authentication and reauthentication].									
SC-12	Cryptographic Key Establishment and Management	When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.		X	X						
SC-13	Use of Cryptography	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.									
SC-14	Public Access Protections	The information system protects the integrity and availability of publicly available information and applications.	X	X	X						
SC-15	Collaborative Computing	The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.		X	X						
SC-15.1		The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.									
SC-16	Transmission of Security Parameters	The information system reliably associates security parameters with information exchanged between information systems.									
SC-17	Public Key Infrastructure Certificates	The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.		X	X						
SC-18	Mobile Code	The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes,		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
		monitors, and controls the use of mobile code within the information system.									
SC-19	Voice Over Internet Protocol	The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.		X	X						
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.		X	X						
SC-20.1		The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.									
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.			X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SC-21.1		The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.									
SC-22	Architecture and Provisioning for Name/Address Resolution Service	The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.		X	X						
SC-23	Session Authenticity	The information system provides mechanisms to protect the authenticity of communications sessions.		X	X						

Security Control Family: System and Information Integrity (SI)

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SI-1	System and Information Integrity Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	X	X	X						
SI-2	Flaw Remediation	The organization identifies, reports, and corrects information system flaws.	X	X	X						
SI-2.1		The organization centrally manages the flaw remediation process and installs updates automatically.			X						
SI-2.2		The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.		X	X						
SI-3	Malicious Code Protection	The information system implements malicious code protection.	X	X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SI-3.1		The organization centrally manages malicious code protection mechanisms.		X	X						
SI-3.2		The information system automatically updates malicious code protection mechanisms.		X	X						
SI-4	Information System Monitoring Tools and Techniques	The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.		X	X						
SI-4.1		The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.									
SI-4.2		The organization employs automated tools to support near-real-time analysis of events.			X						
SI-4.3		The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.									
SI-4.4		The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.		X	X						

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SI-4.5		The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [*Assignment*: organization-defined list of compromise indicators].			X						
SI-5	Security Alerts and Advisories	The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	X	X	X						
SI-5.1		The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.			X						
SI-6	Security Functionality Verification	The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [*Assignment*: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.			X						
SI-6.1		The organization employs automated mechanisms to provide notification of failed automated security tests.									

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SI-6.2		The organization employs automated mechanisms to support management of distributed security testing.									
SI-7	Software and Information Integrity	The information system detects and protects against unauthorized changes to software and information.			X						
SI-7.1		The organization reassesses the integrity of software and information by performing [*Assignment*: organization-defined frequency] integrity scans of the system.			X						
SI-7.2		The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.			X						
SI-7.3		The organization employs centrally managed integrity verification tools.									
SI-8	Spam Protection	The information system implements spam protection.		X	X						
SI-8.1		The organization centrally manages spam protection mechanisms.			X						
SI-8.2		The information system automatically updates spam protection mechanisms.									

Security Control #	Security Control Name	Security Control and Enhancements	Baseline Applicability			Security Control Type	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness	Assessment Steps Used	Assessment Evidence
			L	M	H						
SI-9	Information Input Restrictions	The organization restricts the capability to input information to the information system to authorized personnel.		X	X						
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	The information system checks information for accuracy, completeness, validity, and authenticity.		X	X						
SI-11	Error Handling	The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.		X	X						
SI-12	Information Output Handling and Retention	The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.		X	X						