Nuclear Regulatory Commission
Computer Security Office
Subsystem Security Plan Template

Office Instruction:	**CSO-TEMP-2006**
Office Instruction Title:	**Subsystem Security Plan Template**
Revision Number:	**2.0**
Issuance Date:	**June 11, 2015**
Effective Date:	**June 15, 2015**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PCT**
Description:	CSO-TEMP-2006, "Subsystem Security Plan Template," provides the template used for documenting the specific security controls for which a subsystem is responsible for implementing.
Training:	As requested
ADAMS Accession No.:	ML15133A297

Concurrences			
Primary Office Owner	Policy, Compliance, and Training		
Responsible SITSO	Kathy Lyons-Burke		**Date of Concurrence**
Directors	CSO	Tom Rich (J. Feibus for)	**01-Jun-15**
	PCT	Kathy Lyons-Burke	**01-Jun-15**
	CSA	Thorne Graham	**01-Jun-15**

Concurrence Meeting Conducted on 01-Jun-15			
Attendees:	Kathy Lyons-Burke	Jon Feibus	Charles Watkins

Table of Contents

Computer Security Template
CSO-TEMP-2006

Subsystem Security Plan Template

1 Purpose

The purpose of CSO-TEMP-2006, "Subsystem Security Plan" is to provide the template used for documenting the specific security controls for which a subsystem is responsible for implementing. This template serves as a companion document to a main NRC system security plan (SSP) produced using CSO-TEMP-2007, "System Security Plan Template." This front matter and all explanatory information up through the change history table apply to the template only. All template explanatory information must be removed before completing and submitting the subsystem security plan (Sub-SSP). The Sub-SSP title page should be the first page of the completed document.

2 Template Instructions

The template sections are completed by the system owner organization. Placeholders in <blue> in the template should be replaced with the required information and the font color returned to black before submitting the Sub-SSP. The template explanation and instructions should be removed prior to submission.

2.1 Template-Wide Instructions

General placeholders are provided throughout the Sub-SSP and should be replaced with the required information for all occurrences. Placeholders specific only to certain sections are discussed below.

Replace each general placeholder with the following information:

- <Subsystem Name> – Provide the name of the NRC subsystem for which this Sub-SSP is being developed (NRC subsystem).
- <Subsystem Acronym> – Provide the acronym of the NRC subsystem.
- <Sub-SSP Date> – Provide the date this Sub-SSP was completed or last updated. Use the format "Month DD, YYYY."
- <Sub-SSP Version Number> – Provide the latest version number of this Sub-SSP.
- <Office Name> – Provide the name of the organization that owns the NRC subsystem.
- <Office Acronym> – Provide the acronym of the office.
- <Main System Name> - Provide the name of the main NRC system under whose boundary the NRC subsystem falls.
- <Main System Acronym> - Provide the acronym of the main NRC system.

2.1.1 Headers and Footers

After replacing the placeholders in the headers and footers, check each header and footer throughout the Sub-SSP to ensure that the placeholders were populated accurately.

2.2 Title Page

Supply the specified text for each general placeholder on the title page as indicated in the template-wide instructions.

2.3 Document Revision History Page

Supply the specified text for each general placeholder on the document revision history page as indicated in the template-wide instructions.

Revisions must be in chronological order starting with the newest revision as the first row of the table. The initial release of the Sub-SSP should begin with "Version 1.0." Minor changes (e.g., for quarterly updates) should increase the version number by **.1**. Major changes (e.g., for annual updates or following assessments) should increase the version number to the next applicable whole number. Only released versioning should be used. For example, if modifications to the document are made by writers/reviewers before release, they would not be separate versions.

Example:

Initial Release	Version 1.0
Quarterly Update #1	Version 1.1
Quarterly Update #2	Version 1.2
Quarterly Update #3	Version 1.3
Annual Update	Version 2.0
Reauthorization	Version 3.0

- Replace <Revision History Description> with a specific, brief description of the revisions to the Sub-SSP.

  Example:

  Use the phrase "Initial Release" if this is the first version of the Sub-SSP.

  Subsequent releases would be versioned as indicated above.

- Replace <NRC Staff/Office Name / Company Name> with the name(s) of the organization(s) responsible for developing this subsystem security plan.

2.4 Table of Contents Page

Do not modify the table of contents directly. To update the table of contents:

- Press **CTRL+A** to select all text in the document.
- Press the **F9** key.
- In the Update Table of Contents dialog box, click the Update Entire Table option button.

2.5 Executive Summary Section

Supply the specified text for each general placeholder in the executive summary, as indicated in the template-wide instructions.

Using Table ES-1 in the NRC subsystem's approved security categorization report, populate the following information:

- Replace <Confidentiality High Watermark> with the highest confidentiality impact-level value (High, Moderate, Low) of the NRC subsystem.
- Replace <Integrity High Watermark> with the highest integrity impact-level value (High, Moderate, Low) of the NRC subsystem.
- Replace <Availability High Watermark> with the highest availability impact-level value (High, Moderate, Low) of the NRC subsystem.
- Replace <Overall System Security Categorization> with the overall system security categorization of the NRC subsystem.

Table ES- 1: Sub-SSP Control Family Summary

Table ES- 1: Sub-SSP Control Family Summary must be populated after all security control tables in Section 5, Information Subsystem Security Controls, of this template have been completed. Instructions for completing the security control tables are provided in Section 2.10.3, Completing Security Control Tables, below.

Populate Table ES- 1: Sub-SSP Control Family Summary with the following information for each row of NIST security control families:

- Total Selected Controls column. Replace <N> with the total number of controls selected for each control family.
- In Place column. Replace <N> with the total number of controls determined to be in place for each control family.
- Inherited/Common column. Replace <N> with the total number of controls determined to be inherited or common for each control family.
- N/A column. Replace <N> with the total number of controls determined to be not applicable for each control family.

- Planned column. Replace <N> with the total number of controls determined to be planned for each control family.
- RBD column. Replace <N> with the total number of controls determined to be risk-based decisions for each control family.
- Total Risks column. Add the Planned and RBD column totals for each control family, and provide where <N> is shown. Every cell in this column should be in **bold**.
- Column Total row. For each column, add together the column values, and provide the total where <N> is shown. Every cell in this row should be in **bold**.
- Percentage row. Calculate the percentage of compliance for each column by dividing the column total by the total selected controls value. Provide the percentage where <%> is shown. Every cell in this row should be in **bold**.

2.6 Subsystem Information Section

Supply the specified text for each general placeholder in Section 1, Subsystem Information, as indicated in the template-wide instructions.

2.6.1 Information Subsystem Contacts Section

Table 1.1-1: Subsystem Contacts

Populate Table 1.1-1: Subsystem Contacts with the following information:

NOTE: Add additional rows as necessary to include additional system contacts.

- Name column. Replace <First Name> with the first name and <Last Name> with the last name of the information subsystem contact that corresponds with each role in the Role column.
- Role column. Leave the boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Provide additional roles for each contact, if necessary.
- Title column. Leave the boilerplate text. Replace <Contact Office Acronym> with the acronym of the office to which the information subsystem contact belongs. Where applicable, replace <Contact Title> with the title of the information subsystem contact.
- Organization column. Replace <Contact Organization Name> with the name of the organization for which the information subsystem contact works. Replace <Contact Organization Acronym> with the acronym of the organization. Delete the placeholder if there is no acronym for the organization.
- Work Address column. Replace <Work Address> with the full address of the organization for which the information subsystem contact works. For internal NRC contacts, provide the building, the floor, and the room number of the information subsystem contact (e.g., TWFN 02B05).
- Work Email column. Replace <Work Email> with the NRC email address of the information subsystem contact.

- Work Phone column. Replace <Work Phone> with the work phone number of the information subsystem contact. Use the format "nnn-nnn-nnnn."

2.6.2 Information Subsystem Categorization Section

Supply the specified text for each general placeholder in Section 1.2, Information Subsystem Categorization, as indicated in the template-wide instructions.

- Replace <Security Categorization ML#> with the Agencywide Documents Access and Management System (ADAMS) accession number of the NRC subsystem's security categorization report.
- Replace <Security Categorization Approval Date> with the date the Computer Security Office (CSO) approved the NRC subsystem's security categorization. Use the format "Month DD, YYYY."
- Replace <Security Categorization Approval Memo ML#> with the ADAMS accession number of the approval memo for the NRC subsystem's security categorization.

Using Table ES-1 in the NRC subsystem's approved security categorization report, populate the following information:

- Replace <Confidentiality High Watermark> with the highest confidentiality impact-level value (High, Moderate, Low) of the NRC subsystem.
- Replace <Integrity High Watermark> with the highest integrity impact-level value (High, Moderate, Low) of the NRC subsystem.
- Replace <Availability High Watermark> with the highest availability impact-level value (High, Moderate, Low) of the NRC subsystem

2.6.3 Information Subsystem Operational Status Section

Supply the specified text for each general placeholder in Section 1.3, Information subsystem Operational Status, as indicated in the template-wide instructions.

Indicate the operational status of the subsystem. Table 2.6.3-1: Operational Status Descriptions provides a description of each operational status according to NIST 800-18.

Table 2.6.3-1: Operational Status Descriptions

Operational Status	Description
Operational	The system is in production.
Under Development	The system is being designed, developed, or implemented.
Undergoing a Major Modification	The system is undergoing a major conversion or transition.

- Replace <Operational Status> with the appropriate operational status of the NRC subsystem as described above.
- Replace <Description of Operational Status> with a description of the operational status as described above.

2.6.4 General Subsystem Description/Purpose Section

Provide a general description of the function and purpose (e.g., financial analysis, network support for the agency, etc.) of the NRC subsystem where <General Subsystem Description/Purpose> is shown. The description must include a statement of how the subsystem supports the NRC mission. Include the NRC subsystem's business purpose.

2.7 Subsystem Environment Section

Supply the specified text for each general placeholder in Section 2, Subsystem Environment, as indicated in the template-wide instructions.

NOTE: Refer to the main system SSP if necessary.

- Replace <Subsystem Environment Narrative> with a narrative of the NRC subsystem environment specifying at a minimum:
    - the subsystem location (including both primary and alternate (e.g., continuity of operations plan [COOP]) sites);
    - information on the major technology products implemented within the subsystem; and
    - a clear description of the boundary of the subsystem and what components it includes.

Figure 2-1: <Subsystem Acronym> Boundary and Interconnection Diagram

- Replace the sample boundary and interconnection diagram with the most updated version of the NRC subsystem's boundary and interconnection diagram, including subsystem boundary information. All external connections must be shown on the diagram, with particular attention paid to connections to external systems..
- Replace <Subsystem Diagram Narrative> with a narrative describing the NRC subsystem diagram. The narrative must provide an adequate description of the information shown in the diagram and must include a statement clearly describing the boundary of the subsystem and what components it includes.

  NOTE: No significant information (such as subsystem boundaries) should be conveyed exclusively through the use of color, as the document may be printed in black and white.

  Example:

  Users access the NRC subsystem by connecting to the XYZ Web server using hypertext transfer protocol secure (HTTPS) with the Internet browser installed on their workstations. The user workstations are part of the JKL subsystem managed by the Office of ABC. The XYZ Web server stores its application data on a Microsoft SQL Server 2005 database, which is part of the Windows Infrastructure Services system managed by the Office of ABC. The XYZ Web server also connects to the Windows Active Directory and domain name system (DNS) servers, which are also part of the Windows Infrastructure Services system. These servers provide system-level support functions for the NRC subsystem such as server authentication and domain name lookup services. The back-end SQL database is backed up using backup servers that

are part of the Windows Infrastructure Services system. The NRC subsystem interconnects with the user desktops and back-end support servers using the NRC local area network/wide area network (LAN/WAN), which is managed by the Office of ABC.

Figure 2-2: <Subsystem Acronym> Data Flow Diagram

- Replace the sample data flow diagram with the most updated version of the NRC subsystem's data flow diagram.
- Replace <Subsystem Diagram Narrative> with a narrative of the NRC subsystem diagram. The narrative must provide an adequate description of the information shown in the diagram and must include a statement clearly describing the data flow in the NRC subsystem.

  NOTE: No significant information (such as subsystem boundaries) should be conveyed exclusively through the use of color, as the document may be printed in black and white.

  Example:

  End users send authentication information (in the form of usernames and passwords) to the XYZ Web Server. The XYZ Web Server calculates a one-way hash value from the password supplied and compares it against the stored password previously stored for the user on the ABOC database server. If the hash values match, the authentication is successful.

  End users can submit and retrieve project status information using the XYZ Web Server, which stores the information on the ABC database for future retrieval. The XYZ Web Server calculates earned value management (EVM) data based on information stored in the ABC database server and information provided by end users, and provides this EVM data to end users.

2.7.1 Subsystem Inventory Section

Supply the specified text for each general placeholder in Section 2.1, Subsystem Inventory, as indicated in the template-wide instructions.

- Replace <Location of Inventory> with the location of the NRC subsystem's official inventory. If applicable, provide a link to the NRC subsystem's inventory document.

2.7.2 Subsystem Interconnections / Information Sharing

This information should be contained in the main system SSP.

2.8 Related Laws / Regulations Section

The related laws and regulations provided in this template are common across most NRC systems for the development of the subsystem security plan. If applicable, augment this list with other laws and regulations that were used in the development of this subsystem security plan.

2.9 References Section

Provide additional artifacts that were referenced in this subsystem security plan where <Subsystem Security Artifacts> is shown. Include the title, version number, and ADAMS accession number for each artifact.

2.10 Information Subsystem Security Controls Section

Supply the specified text for each general placeholder in Section 5, Information Subsystem Security Controls, as indicated in the template-wide instructions.

2.10.1 Tailoring Security Controls

Section 5, Information Subsystem Security Controls, contains the security controls cataloged in NIST SP 800-53, Appendix F for non-National Security Systems (NSS) systems. The security controls and enhancements in this section must be tailored according to the NRC subsystem's overall confidentiality, integrity, and availability impact levels (see Section 1.2, Information Subsystem Categorization, in this subsystem security plan for information concerning the NRC subsystem's security categorization). Controls that are common among numerous systems or within the agency should also be identified and documented in the plan. Refer to CSO-STD-0021, "Common and Hybrid Security Control Standard," for additional details concerning common controls.

NOTE: Program management and privacy control families cannot be tailored. NRC subsystems must address these control families regardless of their overall confidentiality, integrity, and availability impact levels.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 rev 4 controls table broken out by confidentiality, integrity, and availability provides a security control tailoring baseline[1], which must be used in order to tailor the security controls and enhancements in Section 5, Information Subsystem Security Controls.

To tailor the security controls:

1. Refer to Section 1.2, Information Subsystem Categorization, of this subsystem security plan for the NRC subsystem's impact levels for confidentiality, integrity, and availability (CIA).
2. Use the controls table and the NRC subsystem's overall CIA impact levels to determine if the security controls and enhancements provided in Section 5, Information Subsystem Security Controls, are applicable to the NRC subsystem's security baseline.
3. Delete any security controls and/or enhancements that are not applicable to the NRC subsystem. Do not delete the entire security control table if the main control is still applicable. Security control enhancements alone may be deleted if they are not applicable to the NRC subsystem.

---

[1] *Source*: CSO website http://nrcweb.nrc.gov:8600/CSO/documents/SP800-53_Rev4_Control_Table.pdf

Examples:

NRC Subsystem 1 – Evaluating CP-7, Alternate Processing Site

NRC Subsystem 1 has an overall subsystem security categorization of Moderate. The impact levels were determined as follows:

- Confidentiality = Moderate
- Integrity = Moderate
- Availability = Low

The controls table shows that CP-7 is only applicable to systems with an availability impact level of moderate or high; CP-7 is not applicable for NRC systems with a low availability impact level. Therefore, even though the overall categorization of the system is moderate, the CP-7 control table in Section 5, Information Subsystem Security Controls, should be deleted from the Sub-SSP template.

NRC Subsystem 2 – Evaluating CA-3 (5), System Interconnections | Restrictions on External System Connections

NRC Subsystem 2 has an overall subsystem security categorization of Moderate. The impact levels were determined as follows:

- Confidentiality = Moderate
- Integrity = Low
- Availability = Moderate

The controls table shows that CA-3 (5) is only applicable to systems with an integrity impact level of moderate or high; CA-3 (5) is not applicable for NRC systems with a low integrity impact level. Therefore, the rows for the CA-3 (5) enhancement in Section 5, Information Subsystem Security Controls, should be deleted from the subsystem security plan template. The entire CA-3 control table should remain in this example because CA-3 (M) ***is*** applicable for NRC systems with a low integrity.

2.10.2 Inherited Security Controls Section

Supply the specified text for each general placeholder in the Section 5.1, Inherited Security Controls, as indicated in the template-wide instructions. These controls should be removed from the information subsystem security controls section.

Table 5.1-1: Inherited Security Controls

For each NIST security control inherited by the main NRC system, populate Table 5.1-1: Inherited Security Controls with the following information:

- NIST Control ID column. Replace <NIST Control ID> with the security control identifier.

- Control Name column. Replace <NIST Control Name> with the name of the security control.
- Description of Inheritance column. Replace <Description of Inheritance> with an overview of how the main NRC system implements the security control **for the NRC subsystem**. Specific details concerning the implementation of the security control are provided in the main NRC system's SSP.

Example:

NIST Control ID	Control Name	Description of Inheritance
AC-1	Access Control Policy and Procedures	The main NRC system develops and reviews/updates the policies and procedures for the NRC subsystem.
CA-2	Security Assessments	The main NRC system is responsible for coordinating all security control testing activities, including the development of security assessment plans, the testing of the security controls in the subsystem, and the production of the security assessment report.

2.10.3 Completing Security Control Tables

The following sections of each security control table in 5.2, is boilerplate text derived from NIST 800-53 Revision 4, and should not be modified:

- Implementation Priority
- Control Type (with the exception of common controls – *see note below*)
- Main Control (shaded row)
- Enhancement (shaded row)

The Main Control and Enhancement sections include the security control objectives with which the NRC subsystem must comply. Red, italicized text in these sections are placeholders for specific values that have been defined by CSO to supplement each security control objective.[2]

NOTE: Do not modify the control type field for hybrid or system specific controls. For common controls, replace <Common> with "System Specific" if the common control is not applicable to the NRC subsystem. For example, a subsystem that is not hosted in an NRC facility cannot rely on certain agency-provided physical protections. Those protections must be provided by the organization owning the NRC subsystem. Refer to CSO-STD-0021, "Common and Hybrid Security Control Standard," for common control applicability.

For each NIST SP 800-53 security control and enhancement table, provide the following:

[2] *Source*: CSO-STD-0020, "Organization Defined Values for System Security Controls"

- Main Control Implementation Detail section. Replace <Main Control Implementation Detail> with a description of the how the control is implemented by the organization or NRC system. Provide detail for each NIST 800-53 objective described in the security control. Implementation detail must be provided for each subsystem that relies on the main system for control implementation. Include all organization and agency policies, directives, or other documentation associated with the implementation of the control. Include all weaknesses discovered during recent assessments (i.e., system cybersecurity assessments) or continuous monitoring activities.
- Control Enhancement Implementation Detail. Replace <Control Enhancement Implementation Detail> with a description of the how the enhancement is implemented by the organization or NRC subsystem. Provide detail for each NIST 800-53 objective described in the security control enhancement. Implementation detail must be provided for each subsystem that relies on the main system for control implementation. Include all organization and agency policies and directives associated with the implementation of the enhancement. Include all weaknesses discovered during recent assessments (i.e., system cybersecurity assessments) or continuous monitoring activities.
- Assessed Status. Evaluate the detail provided in the main control implementation detail and control enhancement implementation detail (if applicable) to determine the assessed status.

  Replace <Assessed Status> with one of the following options:

  - Not Applicable. The control, in its entirety, does not apply to the subsystem because it is specific to technologies that are not implemented within the subsystem.
  - In Place. The control, in its entirety, is implemented with no significant deficiencies.
  - Planned. The control, or any portion of the control, is not currently implemented, but the information subsystem owner plans to implement the control within the current authorization cycle or request a deviation.
  - Risk Based Decision. The control, or a portion of the control, is not implemented, but the authorizing official has accepted the risk of not implementing it or resolving its deficiencies, because it is not feasible to implement the control, or because adequate compensating controls are in place to sufficiently mitigate the risks. Provide a citation for all official deviation or waiver approval memos that support this assessed status. Refer to the most recent CSO deviation/waiver request process (CSO-PROS-1324) for additional information.
  - Provided at Agency Level. The control, in its entirety, is a common control provided by the agency. Provide a citation for any agency guidance or policies that support this assessed status.
  - Provided by <Providing System>. The control, in its entirety, is inherited from another system. Provide a citation for all NRC system agreements (service level agreements [SLAs], memorandums of understanding [MOUs], or interconnection security agreements [ISAs]) that support this assessed status.

  NOTE: It is possible for more than one assessed status to be applicable for any given control or control enhancement. For example, the organization may implement a portion of the control and rely on the agency for another portion of the control. In these cases, the responsibilities of all providing entities must be clearly documented

for each control and/or control enhancement, and for each subsystem (if applicable). Refer to CSO-STD-2102, “System Cybersecurity Assessment Process,” for instructions on how to resolve different statuses within a control table.

CSO-TEMP-2006 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
11-Jun-15	2.0	Repurposed the moderate SSP template as the subsystem SSP template.	Posting to CSO web page and distribution to the ISSO forum	Upon request.

U.S. Nuclear Regulatory Commission

Subsystem Security Plan
<Subsystem Name> (<Subsystem Acronym>)
<Office Name> (<Office Acronym>)

Subsystem of <Main System Name> (<Main System Acronym>)
<Office Name> (<Office Acronym>)

Version <Sub-SSP Version Number>
<Sub-SSP Date>

Document Revision History

Date	Version	Description	Author
<Sub-SSP Date>	<Sub-SSP Version Number>	<Revision History Description>	<NRC Staff/Office Name/ Company Name>

Table of Contents

Executive Summary

<Subsystem Name> (<Subsystem Acronym>) is a subsystem of the <Main System Name> (<Main System Acronym>) system. This Subsystem Security Plan (Sub-SSP) was prepared to accompany the <Main System Acronym> System Security Plan, and provides the specific security controls for which <Subsystem Acronym> is responsible for implementing. Refer to the <Main System Acronym> SSP for the implementation details <Subsystem Acronym> relies on <Main System Acronym> to provide.

As noted in the <Subsystem Acronym> Security Categorization Report, <Subsystem Acronym> has been categorized as a <Overall Subsystem Security Categorization> impact-level system. The evaluated impact levels for confidentiality, integrity, and availability were determined as follows:

Confidentiality = <Confidentiality High Watermark>

Integrity = <Integrity High Watermark>

Availability = <Availability High Watermark>

Refer to Section 1.2, Information Subsystem Categorization, for more details on the <Subsystem Acronym> Security Categorization.

Table ES- 1: Sub-SSP Control Family Summary provides the recommended security controls that are in place, inherited by another system or the agency, not applicable, planned, or risk-based decisions (RBDs).

Table ES- 1: Sub-SSP Control Family Summary

Control Family	Total Selected Controls[3]	In Place	Inherited/ Common	N/A	Planned	RBD	Total Risks
Access Control (AC)	<N>	<N>	<N>	<N>	<N>	<N>	**<N>**
Authority and Purpose (AP)							
Accountability, Audit, and Risk Management (AR)							
Awareness and Training (AT)							
Audit and Accountability (AU)							
Security Assessment and Authorization (CA)							
Configuration Management (CM)							

[3] Total Selected Controls includes control enhancements (e.g. E1, E2, etc.).

Table ES- 1: Sub-SSP Control Family Summary

Control Family	Total Selected Controls[3]	In Place	Inherited/ Common	N/A	Planned	RBD	Total Risks
Contingency Planning (CP)							
Data Quality and Integrity (DI)							
Data Minimization and Retention (DM)							
Identification and Authentication (IA)							
Individual Participation and Redress (IP)							
Incident Response (IR)							
Maintenance (MA)							
Media Protection (MP)							
Physical and Environmental Protection (PE)							
Planning (PL)							
Program Management (PM)							
Personnel Security (PS)							
Risk Assessment (RA)							
System and Services Acquisition (SA)							
System and Communications Protection (SC)							
Security (SE)							
System and Information Integrity (SI)							
Transparency (TR)							
Use Limitation (UL)							
Total	**<N>**	**<N>**	**<N>**	**<N>**	**<N>**	**<N>**	**<N>**
Percentage		**<%>**	**<%>**	**<%>**	**<%>**	**<%>**	**<%>**

1 Subsystem Information

1.1 Subsystem Contacts

Table 1.1-1: Subsystem Contacts

Name	Role	Title	Organization	Work Address	Work Email	Work Phone
<First Name> <Last Name>	Information Subsystem Owner	Director, <Contact Office Acronym>	<Contact Organization Name (<Contact Organization Acronym>)	<Work Address>	<Work Email>	<Work Phone>
	Authorizing Official	Designated Approving Authority				
	Primary Point of Contact	<Contact Title>				
	Backup (Secondary) Point of Contact	<Contact Title>				
	Overall Responsibility of NRC IT Security Program	NRC Chief Information Officer				
	Implementation of NRC IT Security Program	Senior Information Technology Security Officer				
	Overall Responsibility of <Subsystem Acronym> Security	Information subsystem Owner (or Designee)				
	Implementation of <Subsystem Acronym> Security	Information subsystem Security Officer				

1.2 Information Subsystem Categorization

The security categorization of <Subsystem Acronym> has been determined using the guidance of Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information subsystems," and NIST SP 800-60, "Guide for Mapping Types of Information and Information subsystems to Security Categories." The process and results are documented in the <Subsystem Acronym> Security Categorization Report (<Security Categorization ML#>), which was reviewed by the system, subsystem, and information owner. The security categorization report was officially approved on <Security Categorization Approval Date> by the Computer Security Office (CSO). The security categorization approval memo can be found in the Agencywide Documents Access and Management System (ADAMS) at accession number <Security Categorization Approval Memo ML#>.

<Subsystem Acronym> implements the NIST SP 800-53, Revision 4 recommended controls for a system categorized with a <Confidentiality High Watermark> confidentiality level, a <Integrity High Watermark> integrity level, and a <Availability High Watermark> availability level.

1.3 Information subsystem Operational Status

The operational status of <Subsystem Acronym> is <Operational Status>, which means that the subsystem <Description of Operational Status>.

1.4 General Subsystem Description/Purpose

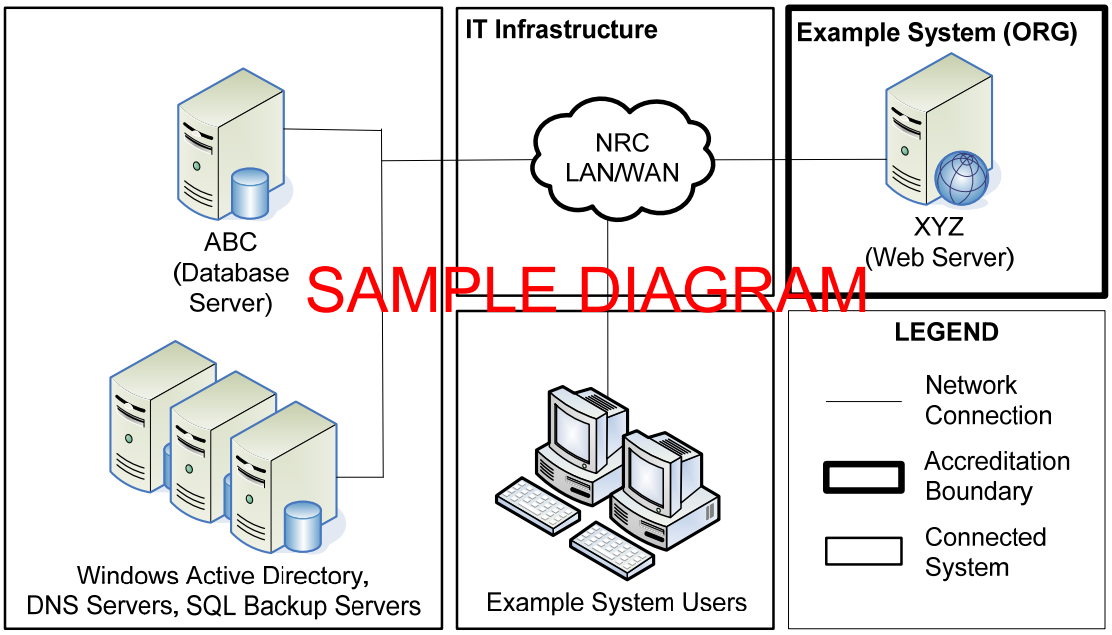
<General Subsystem Description/Purpose>

2 Subsystem Environment

<Subsystem Environment Narrative>

Figure 2-1: <Subsystem Acronym> Boundary and Interconnection Diagram provides a diagram of the <Subsystem Acronym> subsystem boundary and shows the relationship between interconnected systems and subsystems.

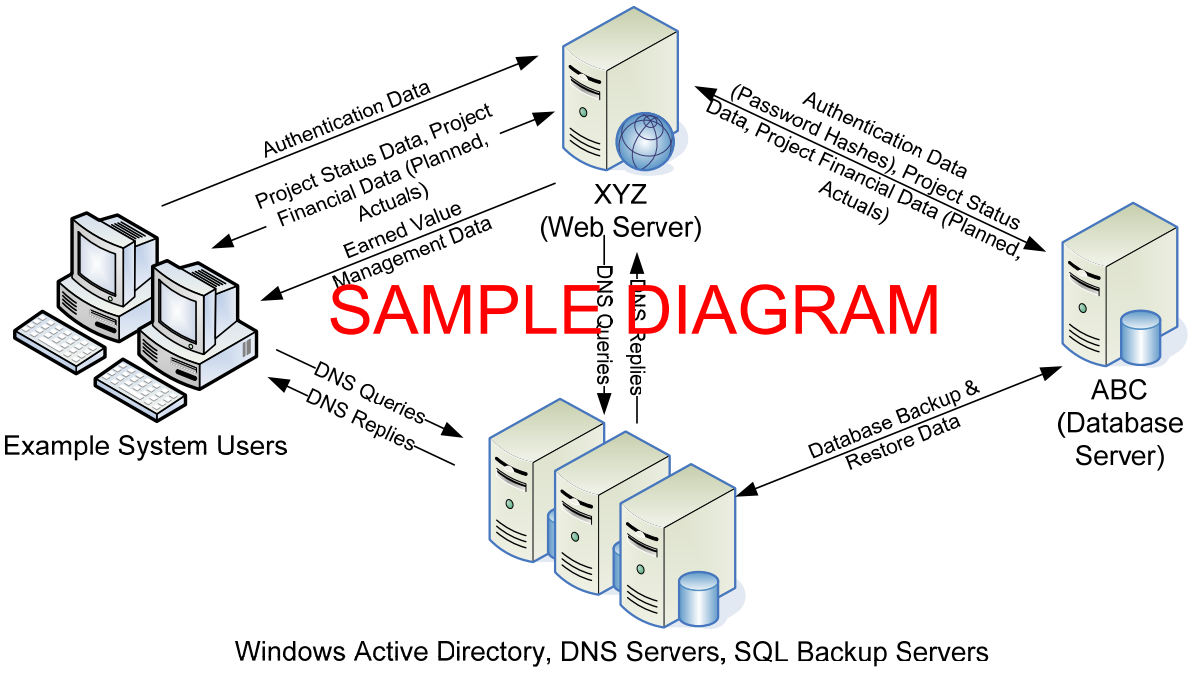
Figure 2-1: <Subsystem Acronym> Boundary and Interconnection Diagram



<Subsystem Diagram Narrative>

Figure 2-2: <Subsystem Acronym> Data Flow Diagram provides a visual representation of the data flow within the subsystem and between interconnected systems and subsystems.

Figure 2-2: <Subsystem Acronym> Data Flow Diagram



<Subsystem Diagram Narrative>

2.1 Subsystem Inventory

The <Subsystem Acronym> inventory document is maintained in <Location of Inventory>. The inventory is updated as subsystem changes occur and is the authoritative source for this information.

3 Related Laws / Regulations

Table 3-1: Related Laws / Regulations provides the related laws and regulations that are pertinent to the development of this Sub-SSP.

Table 3-1: Related Laws / Regulations

Federal Information Security Management Act (FISMA) of 2002	FIPS Publication 140-2, "Security Requirements for Cryptographic Modules," as amended
NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook," as amended	FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information subsystems," as amended
NIST SP 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," as amended	NRC Management Directive 3.53, "NRC Records and Document Management Program," as amended
NIST SP 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," as amended	NRC Management Directive 11.1, "NRC Acquisition of Supplies and Services," as amended
NIST SP 800-30, "Guide for Conducting Risk Assessments," as amended	NRC Management Directive 12.1, "NRC Facility Security Program," as amended
NIST SP 800-34, "Contingency Planning Guide for Federal Information subsystems," as amended	NRC Management Directive 12.3, "NRC Personnel Security Program," as amended
NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information subsystems: A Security Life Cycle Approach," as amended	NRC Management Directive 13.1, "Property Management," as amended
NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," as amended	NRC Volume 10 Management Directives, "Personnel Management/Employment and Staffing," as amended
NIST SP 800-63-2, "Electronic Authentication Guideline," as amended	CSO-PROS-2016, "Plan of Action and Milestones Process," as amended
NIST SP 800-64, "Security Considerations in the System Development Life Cycle," as amended	CSO-PROS-1324, "Deviation Request Process," as amended
NIST SP 800-65, "Integrating IT Security into the Capital Planning and Investment Control Process," as amended	

4 References

- NIST SP 800-18, "Guide for Developing Security Plans for Federal Information subsystems," as amended

- NIST SP 800-53," Security and Privacy Controls for Federal Information subsystems and Organizations," as amended
- NIST SP 800-60, "Guide for Mapping Types of Information and Information subsystems to Security Categories," as amended
- FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information subsystems," as amended
- NRC Management Directive 12.5, "NRC Cyber Security Program," as amended
- CSO-STD-0020, "Organization Defined Values for System Security Controls," as amended
- CSO-STD-0021, "Common and Hybrid Security Control Standard," as amended
- CSO Website for Issuances, http://fusion.nrc.gov/CSO/team/Cyber%20Security%20Issuances/Forms/AllItems.aspx
- <Subsystem Security Artifacts>

5 Information Subsystem Security Controls

Information subsystem security controls were chosen to reflect the <Subsystem Acronym> security baseline with tailoring by confidentiality, integrity, and availability in accordance with the NIST 800-53 Revision 4 control table on the CSO website, http://nrcweb.nrc.gov:8600/CSO/documents/SP800-53_Rev4_Control_Table.pdf. Organization-defined values are depicted in the red italicized text in the applicable test cases. Please refer to CSO-STD-0020, "Organization Defined Values for System Security Controls," and CSO-STD-0021, "Common and Hybrid Security Control Standard," for additional security control responsibilities and requirements.

5.1 Inherited Security Controls

Table 5.1-1: Inherited Security Controls, provides the NIST security controls <Subsystem Acronym> fully inherits from <Main System Acronym>. Refer to the <Main System Acronym> SSP for specific details concerning the control implementation.

Table 5.1-1: Inherited Security Controls

NIST Control ID	Control Name	Description of Inheritance
<NIST Control ID>	<NIST Control Name>	<Description of Inheritance>

5.2 Subsystem Security Controls

The following security controls are the NIST 800-53 controls for which <Subsystem Acronym> cannot rely on <Main System Acronym> to provide.

AC-1 Access Control Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		Hybrid

Main Control: The organization:

a. develops, documents, and disseminates to the [*Chief Information Officer (CIO); Chief Information Security Officer (CISO); Designated Approving Authority (DAA); Information Technology (IT) Executive; IT Manager; IT Functional Manager; IT Systems Development Official; IT Auditor; system owners; information subsystem security officers (ISSOs); office ISSOs; and system administrators (e.g., database, network)*]: (i) an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the access control policy and associated access controls; and

b. reviews and updates [*as needed*] the current: (i) access control policy [*at least annually*]; and (ii) access control procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None

References: NIST Special Publications 880-12, 800-100

Main Control Implementation Detail	**Assessed Status:**	<Assessed Status>
<Main Control Implementation Detail>		

AC-2 Account Management

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. identifies and selects the following types of information subsystem accounts to support organizational missions/business functions:

- [*User: An account used by a single individual regardless of the IT network environment (e.g., development, test, operations/production)*;
- *Privileged User: An account, which is authorized to perform privileged functions, used by a single individual person (e.g., to be used by a system or network administrator).*
- *Shared/Group Account: An account that is used by multiple individuals that require the same access rights and utilize the same, shared authentication credentials.*
- *System: An account used and managed by the operating system and/or applications.*
- *Service: An account that is created explicitly to support services running on a system (e.g., SQLSvc).*
- *Emergency: An account used exclusively by system administrators to perform required actions in the event of an emergency.*
- *Temporary: An account assigned to an individual for a specific purpose for a specified duration*.]

b. assigns account managers for information subsystem accounts;

c. establishes conditions for group and role membership [*in accordance with CSO-STD-2006, "User Access Management Standard*];

d. specifies authorized users of the information subsystem, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account [*in accordance with CSO-STD-2006*];

e. requires approvals by [*system ISSOs*] for requests to create information subsystem accounts;

f. creates, enables, modifies, disables, and removes information subsystem accounts in accordance with [*CSO-STD-2006*];

g. monitors the use of, information subsystem accounts;

h. notifies account managers: (i) when accounts are no longer required; (ii) when users are terminated or transferred; and (iii) when individual information subsystem usage or need-to-know changes;

i. authorizes access to the information subsystem based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions;

- reviews accounts for compliance with account management requirements: [*(i) at least annually for Low sensitivity systems; (ii) at least quarterly for Moderate sensitivity systems; or (iii) at least monthly for High sensitivity systems*]; and

j. establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Supplemental Guidance: Information subsystem account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information subsystems. The identification of authorized users of the information subsystem and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information subsystem accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information subsystem availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information subsystem accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

References: None

Main Control Implementation Detail	**Assessed Status:**	<Assessed Status>
<Main Control Implementation Detail>		

Control Type:	**System-Specific**

Control Enhancement 1: Account Management | Automated System Account Management

The organization employs automated mechanisms to support the management of information subsystem accounts.

Supplemental Guidance: The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information subsystem to monitor account usage; and using telephonic notification to report atypical system account usage.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	<Assessed Status>
<Control Enhancement Implementation Details>		

Control Type:	**System-Specific**	
Control Enhancement 2: Account Management | Removal of Temporary / Emergency Accounts The information subsystem automatically [*removes*] temporary and emergency accounts after: [*(i) no more than 30 days from creation of account for Low sensitivity systems; (ii) no more than 30 days from creation of account for Moderate sensitivity systems; or (iii) no more than 15 days from creation of account for High sensitivity systems*]. Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	<Assessed Status>
<Control Enhancement Implementation Details>		
Control Type:	**Hybrid**	
Control Enhancement 3: Account Management | Disable Inactive Accounts The information subsystem automatically disables inactive accounts after: [*(i) no more than 90 days for Low sensitivity systems; (ii) no more than 90 days for Moderate sensitivity systems; or (iii) no more than 90 days for High sensitivity systems*]. Supplemental Guidance: None		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	<Assessed Status>
<Control Enhancement Implementation Details>		
Control Type:	**System-Specific**	
Control Enhancement 4: Account Management | Automated Audit Actions The information subsystem automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*the system ISSO or designee*]. Supplemental Guidance: Related controls: AU-2, AU-12		
Control Enhancement 4 Implementation Detail	**Assessed Status:**	<Assessed Status>
<Control Enhancement Implementation Details>		
Control Type:	**Hybrid**	
Control Enhancement 5: Account Management | Inactivity Logout The organization requires that users are logged out after [*30 minutes of inactivity unless the session has been locked*]. Supplemental Guidance: Related control: SC-23.		
Control Enhancement 5 Implementation Detail	**Assessed Status:**	<Assessed Status>
<Control Enhancement Implementation Details>		
Control Type:	**System-Specific**	
Control Enhancement 12: Account Management | Account Monitoring / Atypical Usage The organization: a. monitors information subsystem accounts for [*atypical usage such as accessing the system at certain times of the day and from locations that are not consistent with the normal usage patterns of the individual*]; and b. reports atypical usage of information subsystem accounts to the [*Computer Security Incident Response Team (CSIRT) and system ISSO*]. Supplemental Guidance: Atypical usage includes, for example, accessing information subsystems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related control: CA-7.		
Control Enhancement 12 Implementation Detail	**Assessed Status:**	<Assessed Status>
<Control Enhancement Implementation Details>		

Control Type:	**System-Specific**

Control Enhancement 13: Account Management | Disable Accounts for High-Risk Individuals

The organization disables accounts of users posing a significant risk within [*30 minutes*] of discovery of the risk.

Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information subsystems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between authorizing officials, information subsystem administrators, and human resource managers is essential in order for timely execution of this control enhancement. Related control: PS-4.

Control Enhancement 13 Implementation Detail	**Assessed Status:**	<Assessed Status>
<Control Enhancement Implementation Details>		

AC-3 Access Enforcement

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information subsystems. In addition to enforcing authorized access at the information subsystem level and recognizing that information subsystems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.

Control Enhancements: None

References: None

Main Control Implementation Detail	**Assessed Status:**	

AC-4 Information Flow Enforcement

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on:

- [*The characteristics of the information and the information path by enforcing policies through boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls);*
- *Keeping export-controlled information from being transmitted in the clear to the Internet;*
- *Blocking outside traffic that claims to be from within the NRC;*
- *Restricting web requests to the Internet that are not from the internal web proxy server; and*
- *Limiting information transfers between NRC and other organizations based on data structures and content*].

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information subsystem and between information subsystems (as opposed to who is allowed to access the

information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information subsystems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy re-grading mechanisms to reassign security attributes and security labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information subsystems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information subsystem services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements: None

References: None.

Main Control Implementation Detail	**Assessed Status:**	

AC-5 Separation of Duties

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. separates [*information subsystem support functions among different individuals and/or roles*];

b. documents separation of duties of individuals; and

c. defines information subsystem access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information subsystem support functions among different individuals and/or roles; (ii) conducting information subsystem support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None

References: None

Main Control Implementation Detail	**Assessed Status:**	

AC-6 Least Privilege

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information subsystems. The principle of least privilege is also applied to information subsystem processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information subsystem accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information subsystems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

References: None

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Least Privilege | Authorize Access to Security Functions

The organization explicitly authorizes access to the following security functions (deployed in hardware, software, and firmware), and security-relevant information:

- [*Establishing system accounts*
- *Configuring access authorizations (i.e., permissions, privileges)*
- *Setting events to be audited*
- *Setting intrusion detection parameters*
- *Authorizing personnel for the following roles:*
  - *Security administrators*
  - *System administrators*
  - *Network administrators*
  - *ISSOs*
  - *System maintenance personnel*
  - *System programmers*
  - *Other privileged users*].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Least Privilege | Non-Privileged Access for Nonsecurity Functions

The organization requires that users of information subsystem accounts, or roles, with access to [*system accounts, access authorizations, audit records, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists*], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as

role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 3: Least Privilege | Network Access to Privileged Commands The organization authorizes network access to [*privileged commands that change auditing parameters or user/object privileges]* only for [*compelling operational needs that require rapid response (e.g., in response to a security incident)*] and documents the rationale for such access in the security plan for the information subsystem. Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 5: Least Privilege | Privileged Accounts The organization restricts privileged accounts on the information subsystem to [*authorized system administrators and other roles with a specific mission/business need*]. Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information subsystem configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.		
Control Enhancement 5 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 9: Least Privilege | Auditing Use of Privileged Functions The information subsystem audits the execution of privileged functions. Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information subsystem accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.		
Control Enhancement 9 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 10: Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions The information subsystem prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. Supplemental Guidance: Privileged functions include, for example, establishing information subsystem accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.		

Control Enhancement 10 Implementation Detail	Assessed Status:	

AC-7 Unsuccessful Logon Attempts

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem:

a. enforces a limit of [*no more than 3*] consecutive invalid logon attempts by a user during a [*15 minute time period*] and

b. automatically [*locks the account/node*] for [*at least 30 minutes or until unlocked by a system administrator*] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information subsystems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information subsystem components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Enhancements: None

References: None

Main Control Implementation Detail	Assessed Status:	

AC-8 System Use Notification

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The information subsystem:

a. displays to users [*the NRC-approved system use notification in accordance with CSO-STD-0040, "Warning Banner Standard,"*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) Users are accessing a U.S. Government information subsystem; (ii) Information subsystem usage may be monitored, recorded, and subject to audit; (iii) Unauthorized use of the information subsystem is prohibited and subject to criminal and civil penalties; and (iv) Use of the information subsystem indicates consent to monitoring and recording;

b. retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information subsystem; and

c. for publicly accessible systems: (i) displays system use information [*NRC-approved system use notification in accordance with CSO-STD-0040*], before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes a description of the authorized uses of the system.

Supplemental Guidance: System use notifications can be implemented using messages or warning banners displayed before individuals log in to information subsystems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information subsystem users. Organizations also consult with the Office of the

General Counsel for legal review and approval of warning banner content. Control Enhancements: None References: None		
Main Control Implementation Detail	**Assessed Status:**	

AC-10 Concurrent Session Control

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**System-Specific**
Main Control: The information subsystem limits the number of concurrent sessions for each account to: [*(i) 2 concurrent sessions for remote users; (ii) 2 concurrent sessions for non-privileged users; and (iii) 3 concurrent sessions for local privileged users*]. Supplemental Guidance: Organizations may define the maximum number of concurrent sessions for information subsystem accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information subsystem accounts and does not address concurrent sessions by single users via multiple system accounts. Control Enhancements: None References: None		
Main Control Implementation Detail		**Assessed Status:**

AC-11 Session Lock

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**Hybrid**
Main Control: The information subsystem: a. prevents further access to the system by initiating a session lock after [*15 minutes for Low, Moderate, or High sensitivity systems*] of inactivity or upon receiving a request from a user; and b. retains the session lock until the user reestablishes access using established identification and authentication procedures. Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information subsystems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information subsystems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7. References: OMB Memorandum 06-16		
Main Control Implementation Detail		**Assessed Status:**
Control Type:		**Hybrid**
Control Enhancement 1: Session Lock | Pattern-Hiding Displays		

The information subsystem conceals, via the session lock, information previously visible on the display with a publicly viewable image. Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

AC-12 Session Termination

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem automatically terminates a user session after: [*(i) violation of time-of-day restrictions on information subsystem use; (ii) targeted responses to security incidents; or (iii) the maximum permitted user session duration specified for the account has been exceeded.*].

Supplemental Guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information subsystem. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information subsystem use. Related controls: SC-10, SC-23.

Control Enhancements: None

References: None

Main Control Implementation Detail	**Assessed Status:**	

AC-14 Permitted Actions without Identification or Authentication

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. identifies [*a limited number of user actions (e.g., access to publicly available federal information subsystems, use of mobile phones to receive calls, and receiving facsimiles [faxes])*] that can be performed on the information subsystem without identification or authentication consistent with organizational missions/business functions; and

b. documents and provides supporting rationale in the security plan for the information subsystem, user actions not requiring identification, or authentication.

Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational information subsystems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information subsystems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to

situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information subsystems without identification and authentication and thus, the values for assignment statements can be none. Related controls: CP-2, IA-2. Control Enhancements: None References: None

Main Control Implementation Detail	**Assessed Status:**	

AC-17 Remote Access

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. authorizes remote access to the information subsystem prior to allowing such connections.

Supplemental Guidance: Remote access is access to organizational information subsystems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information subsystems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Remote Access | Automated Monitoring / Control

The information subsystem monitors and controls remote access methods.

Supplemental Guidance: Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information subsystem components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 2: Remote Access | Protection of Confidentiality / Integrity Using Encryption

The information subsystem implements cryptographic mechanisms to protect the confidentiality and integrity of

remote access sessions. Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 3: Remote Access | Managed Access Control Points The information subsystem routes all remote accesses through [*a limited number (as specified by the Department of Homeland Security [DHS] Trusted Internet Connections [TIC] initiative requirements)*] of managed network access control points. Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 4: Remote Access | Managed Access Control Points The organization: a. authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*remote maintenance activities external to the NRC network*]; and b. documents the rationale for such access in the security plan for the information subsystem. Supplemental Guidance: Related control: AC-6.		
Control Enhancement 4 Implementation Detail	**Assessed Status:**	

AC-18 Wireless Access

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**Hybrid**	
Main Control: The organization: a. establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. authorizes wireless access to the information subsystem prior to allowing such connections. Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4. References: NIST Special Publications 800-48, 800-94, 800-97.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Wireless Access | Authentication and Encryption The information subsystem protects wireless access to the system using authentication of [*users and devices*] and encryption.		

Supplemental Guidance: Related controls: SC-8, SC-13.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 4: Wireless Access | Restrict Configurations by Users

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information subsystems. Related controls: AC-3, SC-15.

Control Enhancement 4 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 5: Wireless Access | Antennas / Transmission Power Levels

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Supplemental Guidance: Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information subsystems as well as other systems that may be operating in the area. Related control: PE-19.

Control Enhancement 5 Implementation Detail	**Assessed Status:**	

AC-19 Access Control for Mobile Devices

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

b. authorizes the connection of mobile devices to organizational information subsystems.

Supplemental Guidance: A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection,

firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared).

Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.

References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 5: Access Control for Mobile Devices | Full Device / Container-Based Encryption

The organization employs either [*full-device encryption or container encryption*] to protect the confidentiality and integrity of information on [*mobile computing devices*].

Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28.

Control Enhancement 5 Implementation Detail	**Assessed Status:**	

AC-20 Use of External Information subsystems

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information subsystems, allowing authorized individuals to:

a. access the information subsystem from external information subsystems; and

b. process, store, or transmit organization-controlled information using external information subsystems.

Supplemental Guidance: External information subsystems are information subsystems or components of information subsystems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information subsystems include, for example: (i) personally owned information subsystems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information subsystems owned or controlled by nonfederal governmental organizations; and (iv) federal information subsystems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information subsystems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information subsystems.

For some external information subsystems (i.e., information subsystems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information subsystems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel,

contractors, or other individuals with authorized access to organizational information subsystems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

This control does not apply to the use of external information subsystems to access public interfaces to organizational information subsystems (e.g., individuals accessing federal information through www.usa.gov). Organizations establish terms and conditions for the use of external information subsystems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information subsystems from external information subsystems; and the highest security category of information that can be processed, stored, or transmitted on external information subsystems. If terms and conditions with the owners of external information subsystems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. Related controls: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.

References: FIPS Publication 199.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Use of External Information subsystems | Limits on Authorized Use

The organization permits authorized individuals to use an external information subsystem to access the information subsystem or to process, store, or transmit organization-controlled information only when the organization:

a. verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

b. retains approved information subsystem connection or processing agreements with the organizational entity hosting the external information subsystem.

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information subsystems (e.g., contractors, coalition partners) need to access organizational information subsystems. In those situations, organizations need confidence that the external information subsystems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information subsystems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 2: Use of External Information subsystems | Portable Storage Devices

The organization [*restricts*] the use of organization-controlled portable storage devices by authorized individuals on external information subsystems [*in accordance with the "NRC Agency-wide Rules of Behavior for Authorized Computer Use" CSO-STD-2004, "Electronic Media and Device Handling Standard;" and system-specific requirements*].

Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external information subsystems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

AC-21 Information Sharing

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information (e.g., SUNSI, SGI, and classified information) for [*approved information-sharing circumstances where user discretion is required*]; and

b. employs [*automated mechanisms or manual processes (defined in the applicable SSP)*] to assist users in making information sharing/collaboration decisions.

Supplemental Guidance: This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Related control: AC-3.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

AC-22 Publicly Accessible Content

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. designates individuals authorized to post information onto a publicly accessible information subsystem;

b. trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. reviews the proposed content of information prior to posting onto the publicly accessible information subsystem to ensure that nonpublic information is not included; and

d. reviews the content on the publicly accessible information subsystem for nonpublic information [*at least quarterly or as new information is posted*] and removes such information, if discovered.

Supplemental Guidance: In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information subsystems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information subsystems is covered by organizational policy. Related controls: AC-3, AC-4, AT-2, AT-3, AU-13.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

AP-1 Authority to Collect

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control:

The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information subsystem need.

Supplemental Guidance: Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements. Related controls: AR-2, DM-1, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Circular A-130, Appendix I.

Main Control Implementation Detail	**Assessed Status:**	

AP-2 Purpose Specification

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control:

The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Supplemental Guidance: Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice. Related controls: AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B); Sections 208(b), (c), E-Government Act of 2002 (P.L. 107-347).

Main Control Implementation Detail	**Assessed Status:**	

AR-1 Governance and Privacy Program

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information subsystems;

b. monitors federal privacy laws and policy for changes that affect the privacy program;

c. allocates [*budget and staffing*] sufficient resources to implement and operate the organization-wide privacy program;

d. develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;

e. develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information subsystems, or technologies involving PII; and

f. updates privacy plan, policies, and procedures [*at least every 2 years*].

Supplemental Guidance: The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.

To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 07-16; OMB Circular A-130; Federal Enterprise Architecture Security and Privacy Profile.

Main Control Implementation Detail	**Assessed Status:**	

AR-2 Privacy Impact and Risk Assessment

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and

b. conducts Privacy Impact Assessments (PIAs) for information subsystems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Supplemental Guidance: Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct

of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information subsystems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information subsystems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information subsystems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

Control Enhancements: None.

References: Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 10-23.

Main Control Implementation Detail	**Assessed Status:**	

AR-3 Privacy Requirements for Contractors and Service Providers

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. includes privacy requirements in contracts and other acquisition-related documents.

Supplemental Guidance: Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information subsystems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information subsystems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information subsystems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

Control Enhancements: None.

References: Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 10-23.

Main Control Implementation Detail	**Assessed Status:**	

AR-4 Privacy Monitoring and Auditing

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control:

The organization monitors and audits privacy controls and internal privacy policy [*at least every 2 years*] to ensure effective implementation.

Supplemental Guidance: To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance

gaps identified in programs, projects, and information subsystems. In addition to auditing for effective implementation of all privacy controls identified in this appendix, organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information subsystems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information subsystems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).

Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials. Related controls: AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 05-08, 06-16, 07-16; OMB Circular A-130.

Main Control Implementation Detail	**Assessed Status:**	

AR-5 Privacy Awareness and Training

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. administers basic privacy training [*at least annually*] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [*at least annually*]; and

c. ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [*at least annually*].

Supplemental Guidance: Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as Privacy Impact Assessments (PIAs) or System of Records Notices (SORNs) for a program or information subsystem. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, program, business process, and information subsystem requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training. Related controls: AR-3, AT-2, AT-3, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(e); Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.

Main Control Implementation Detail	**Assessed Status:**	

AR-6 Privacy Reporting

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control:

The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Supplemental Guidance: Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Agency Official for Privacy (SAOP) reports to OMB; (ii) reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; and (iii) other public reports required by specific statutory mandates or internal policies of organizations. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 803, 9/11 Commission Act, 42 U.S.C. § 2000ee-1; Section 804, 9/11 Commission Act, 42 U.S.C. § 2000ee-3; Section 522, Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Memoranda 03-22; OMB Circular A-130.

Main Control Implementation Detail	**Assessed Status:**	

AR-7 Privacy-Enhanced System Design and Development

Implementation Priority:	N/A	N/A
Control Type:		**System-Specific**

Main Control:

The organization designs information subsystems to support privacy by automating privacy controls.

Supplemental Guidance: To the extent feasible, when designing organizational information subsystems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information subsystem breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization's privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information subsystem use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes. Related controls: AC-6, AR-4, AR-5, DM-2, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10); Sections 208(b) and(c), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22.

Main Control Implementation Detail	**Assessed Status:**	

AR-8 Accounting of Disclosures

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (i) date, nature, and purpose of each disclosure of a record; and (ii) name and address of the person or agency to which the disclosure was made;

b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

c. Makes the accounting of disclosures available to the person named in the record upon request.

Supplemental Guidance: The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals. Related control: IP-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k).

Main Control Implementation Detail	**Assessed Status:**	

AT-1 Security Awareness and Training Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to the [*Chief Information Officer (CIO); Chief Information Security Officer (CISO); Director, Office of the Chief Human Capital Officer (OCHCO); office directors, Information Technology (IT) coordinators, information subsystem security officers (ISSOs), regional administrators, and front-line supervisors; and authenticated users of NRC information subsystems; and, the following personnel with the following roles: CIO; CISO; Designated Approving Authority [DAA]; IT executive; IT manager; IT functional manager; IT systems development official; IT auditors; system owners; system ISSO; database administrators; network administrators; and system administrators*]: (i) a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

b. reviews and updates [*as needed*] the current: (i) Security awareness and training policy [*annually*]; and (ii) security awareness and training procedures [*annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.		
Main Control Implementation Detail	**Assessed Status:**	

AT-2 Security Awareness Training

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization provides basic security awareness training to information subsystem users (including managers, senior executives, and contractors):

a. as part of initial training for new users;

b. when required by information subsystem changes; and

c. [*at least annually*] thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information subsystems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); Executive Order 13587; NIST Special Publication 800-50.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**<Common>**

Control Enhancement 2: Security Awareness | Insider Threat

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PM-12, PS-3, PS-6.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

AT-3 Role-Based Security Training

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. before authorizing access to the information subsystem or performing assigned duties;

b. when required by information subsystem changes; and

c. [*In accordance with the NRC Cyber Security Workforce Development Training Plan*] thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information subsystems to which personnel have authorized access. In addition, organizations provide enterprise architects, information subsystem developers, software developers, acquisition/procurement officials, information subsystem managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

Control Enhancements: None.

References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); NIST Special Publications 800-16, 800-50.

Main Control Implementation Detail	**Assessed Status:**	

AT-4 Security Training Records

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. documents and monitors individual information subsystem security training activities including basic security awareness training and specific information subsystem security training; and

b. retains individual training records [*in accordance with MD 3.53, "NRC Records and Document Management Program" Handbook 1, "NRC Records Management Program."*].

Supplemental Guidance: Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

AU-1 Audit and Accountability Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to the [*CIO; CISO; DAA; IT executive; IT manager; IT functional manager; IT systems development official; IT auditor; system owners; ISSOs; office ISSOs; and system administrators (e.g., database, network)*]: (i) an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the audit and accountability policy and associated audit and

accountability controls; and

b. reviews and updates [*as needed*] the current: (i) audit and accountability policy [*at least annually*]; and (ii) audit and accountability procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

AU-2 Audit Events

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. determines that the information subsystem is capable of auditing the following events: [*all events specified in CSO-STD-2005, "System Monitoring Standard," for unclassified systems*];

b. coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. determines that the following events are to be audited within the information subsystem: [*all events identified in CSO-STD-2005, as required for all systems, for the system's Federal Information Processing Standard (FIPS) 199 level*].

Supplemental Guidance: An event is any observable occurrence in an organizational information subsystem. Organizations identify audit events as those events which are significant and relevant to the security of information subsystems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information subsystems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information subsystem needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information subsystems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

References: NIST Special Publication 800-92; Web: http://idmanagement.gov.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**
Control Enhancement 3: Audit Events | Reviews and Updates The organization reviews and updates the audited events [*at least annually*]. Supplemental Guidance: Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.	

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

AU-3 Content of Audit Records

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**
Main Control: The information subsystem generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information subsystem after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11. References: None.		

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**
Control Enhancement 1: Content of Audit Records | Additional Audit Information The information subsystem generates audit records containing the additional information: [*specified in CSO-STD-2005*]. Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.	

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**
Control Enhancement 2: Content of Audit Records | Centralized Management of Planned Audit Record Content The information subsystem provides centralized management and configuration of the content to be captured in audit records generated by: - [*Firewalls* - *Security devices/appliances* - *Core routers/border routers*	

- *Domain controllers*
- *Domain Name System (DNS) servers*
- *Critical servers and workstations that provide essential system or agency services, which are specified in the system Business Impact Analysis [BIA]*].

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information subsystem. Related controls: AU-6, AU-7.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

AU-4 Audit Storage Capacity

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization allocates audit record storage capacity in accordance with the [*National Archives and Records Administration (NARA) and NRC defined audit record retention requirements;* and configures [*primary audit record storage capacity to support audit record storage for the following durations: (i) at least 2 calendar weeks for Low sensitivity systems; (ii) at least 3 calendar months for Moderate sensitivity systems; and (iii) at least 1 calendar year for High sensitivity systems*].

Supplemental Guidance: Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

AU-5 Response to Audit Processing Failures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem:

a. alerts the [*system ISSO and system administrator*] in the event of an audit processing failure; and

b. takes the following additional actions:

- [*For audit processing failures due to insufficient storage available:*
  - *Overwrites oldest audit records for Low sensitivity systems*
  - *Overwrites oldest audit records for Moderate sensitivity systems*
  - *Overwrites oldest audit records for High sensitivity systems*
- *For other audit processing failures (e.g., errors in transmitting, receiving, processing audit records and information):*
  - *Restarts or restores affected services or system components to ensure that audit processing failures are resolved.*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to

define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information subsystem component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12. References: None.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Response to Audit Processing Failures | Audit Storage Capacity The information subsystem provides a warning to [*the system ISSO and system administrator*] within [*1 calendar day*] when allocated audit record storage volume reaches [*60%*] of repository maximum audit record storage capacity. Supplemental Guidance: Organizations may have multiple audit data storage repositories distributed across multiple information subsystem components, with each repository having different storage volume capacities.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Response to Audit Processing Failures | Real-Time Alerts The information subsystem provides a real-time alert to [*the system ISSO and system administrator*] when the following audit failure events occur: [*(i) when 60% of maximum audit storage (and every additional 10% thereafter) is achieved; (ii) when the audit file is deleted or individual audit records are modified; (iii) when the audit file permissions are modified; and (iv) if the audit record repository has not received audit records*]. Supplemental Guidance: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	

AU-6 Audit Review, Analysis, and Reporting

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**System-Specific**	
Main Control: The organization: a. reviews and analyzes information subsystem audit records for indications of inappropriate or unusual activity, including indicators of compromise: [*(i) at least hourly on High sensitivity systems; (ii) at least daily on Low and Moderate sensitivity systems; or (iii) at least quarterly on stand-alone systems (not connected to the Internet or production network).*] b. reports findings to [*the system ISSO and system administrator*]. Supplemental Guidance: Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information subsystem boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.		

References: None.		
Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Audit Review, Analysis, and Reporting | Process Integration

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 3: Audit Review, Analysis, and Reporting | Correlate Audit Repositories

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information subsystem) and supports cross-organization awareness. Related controls: AU-12, IR-4.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 5: Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities

The organization integrates analysis of audit records with analysis of [*configuration and vulnerability scanning information, performance data, and information subsystem monitoring information*] to further enhance the ability to identify inappropriate or unusual activity.

Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or information subsystem monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple information subsystem components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can help uncover denial of service attacks or cyber-attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations. Related controls: AU-12, IR-4, RA-5.

Control Enhancement 5 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 6: Audit Review, Analysis, and Reporting | Correlation with Physical Monitoring

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Supplemental Guidance: The correlation of physical audit information and audit logs from information subsystems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identify for logical access to certain information subsystems with the

additional physical security information that the individual was actually present at the facility when the logical access occurred, may prove to be useful in investigations.		
Control Enhancement 6 Implementation Detail	**Assessed Status:**	

AU-7 Audit Reduction and Report Generation

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem provides an audit reduction and report generation capability that:

a. supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

b. does not alter the original content or time ordering of audit records.

Supplemental Guidance: Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information subsystem or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information subsystem can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Audit Reduction and Report Generation | Automatic Processing

The information subsystem provides the capability to process audit records for events of interest based on [*the list of auditable events identified in AU-3 (1) Additional Audit Information*].

Supplemental Guidance: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or sub-network) or selectable by specific information subsystem component. Related controls: AU-2, AU-12.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

AU-8 Time Stamps

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem:

a. uses internal system clocks to generate time stamps for audit records; and

b. records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and are synchronized [*within plus or minus 1 minute*].

Supplemental Guidance: Time stamps generated by the information subsystem include date and time. Time is

commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information subsystem clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12. References: None.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Time Stamps | Synchronization with Authoritative Time Source The information subsystem: a. compares the internal information subsystem clocks [*daily*] with [*NRC designated time servers that obtain time from the Naval Observatory Master Clock.*]; and b. synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*1 minute*]. Supplemental Guidance: This control enhancement provides uniformity of time stamps for information subsystems with multiple system clocks and systems connected over a network.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

AU-9 Protection of Audit Information

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**System-Specific**	
Main Control: The information subsystem protects audit information and audit tools from unauthorized access, modification, and deletion. Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information subsystem activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6. References: None.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Protection of Audit Information | Audit Backup on Separate Physical Systems / Components The information subsystem backs up audit records [*at the same time as other system information back-ups*] onto a physically different system or system component than the system or component being audited. Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information subsystem being audited does not also result in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11.		

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 3: Protection of Audit Information | Cryptographic Protection

The information subsystem implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Supplemental Guidance: Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash. Related controls: AU-10, SC-12, SC-13.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 4: Protection of Audit Information | Access by Subset of Privileged Users

The organization authorizes access to management of audit functionality to only [*system ISSOs, system administrators designated within the SSP, CSO personnel, Office of the Inspector General (OIG) Investigations Cyber Crime Unit (CCU) personnel*].

Supplemental Guidance: Individuals with privileged access to an information subsystem and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5.

Control Enhancement 4 Implementation Detail	**Assessed Status:**	

AU-10 Audit Storage Capacity

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.

Control Type:	**System-Specific**

Main Control: The information subsystem protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*actions that require non-repudiation as specified in the SSP*].

Supplemental Guidance: Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Related controls: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

AU-11 Audit Record Retention

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**System-Specific**

Main Control: The organization retains [*in accordance with NARA General Records Schedule (GRS); 20, Electronic Records, and MD 3.53*] audit records for [*the duration of the investigation and for the legally required timeframe after the investigation is complete*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

AU-12 Audit Generation

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem:

a. provides audit record generation capability for the auditable events defined in AU-2.a. for [*all information subsystems components and network components, such as: (i) firewalls; (ii) domain controllers; (iii) workstations (desktop PCs and laptops); (iv) servers; (v) security devices; (vi) network devices (routers, switches); and (vii) Virtual Private Network (VPN) devices]*;

b. allows [*system owners and system ISSOs*] to select which auditable events are to be audited by specific components of the information subsystem; and

c. generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Supplemental Guidance: Audit records can be generated from many different information subsystem components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information subsystem is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Audit Generation | Time-Correlated Audit Trail

The information subsystem compiles audit records from [*firewalls, domain controllers, workstations (desktop PCs and laptops), servers, security devices, network devices (routers, switches), VPN devices*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*plus or minus 1 minute*].

Supplemental Guidance: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances. Related controls: AU-8, AU-12.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 3: Audit Generation | Changes by Authorized Individuals

The information subsystem provides the capability for [*only system ISSOs and authorized system administrators*] to change the auditing to be performed on [*the information subsystem components defined in AU-12 (1) System Wide / Time Correlated Audit Trail*] based on [*an urgent need, such as an incident or threat situation*] within [*near-real time thresholds*].

Supplemental Guidance: This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information subsystem resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours. Related control: AU-7.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

CA-1 Security Assessment and Authorization

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. Develops, documents, and disseminates to [*Chief Information Officer (CIO); Chief Information Security Officer (CISO); Designated Approving Authority (DAA); Director, Office of Information Services (OIS); system information subsystem security officers (ISSOs); and system owners*]: (i) a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls;

b. Reviews and updates [*as needed*] the current: (i) security assessment and authorization policy [*at least annually*]; and (ii) security assessment and authorization procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

CA-2 Security Assessments

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops a security assessment plan that describes the scope of the assessment including: (i) security controls and control enhancements under assessment; (ii) assessment procedures to be used to determine security control effectiveness; and (iii) assessment environment, assessment team, and assessment roles and responsibilities;

b. assesses the security controls in the information subsystem and its environment of operation [*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 established security requirements;

c. produces a security assessment report that documents the results of the assessment; and

d. provides the results of the security control assessment to the [*CISO; CSO Senior Information Technology Security Officer (SITSO) with responsibility for continuous monitoring oversight; system ISSO; and DAA*].

Supplemental Guidance: Organizations assess security controls in organizational information subsystems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information subsystems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information subsystems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information subsystem authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

References: Executive Order 13587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Security Assessments | Independent Assessors

The organization employs assessors or assessment teams with [*the required skills, experience, and technical expertise for conducting an impartial assessment of security controls employed within or inherited by the information*

subsystem] to conduct security control assessments.

Supplemental Guidance: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information subsystems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information subsystems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information subsystems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information subsystem owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information subsystems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**<Common>**

Control Enhancement 2: Security Assessments | Specialized Assessments

The organization includes as part of security control assessments for high-sensitivity systems, [*annual*; *announced and unannounced*; *in-depth monitoring, malicious user testing, penetration testing, or red team exercises*].

Supplemental Guidance: Organizations can employ information subsystem monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

CA-3 System Interconnections

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. authorizes connections from the information subsystem to other information subsystems through the use of interconnection security agreements;

b. documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. reviews and updates interconnection security agreements [*at least annually and whenever there is a change to the interconnection*].

Supplemental Guidance: This control applies to dedicated connections between information subsystems (i.e., system

interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information subsystems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information subsystem connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information subsystems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

References: FIPS Publication 199; NIST Special Publication 800-47.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 5: System Interconnections | Restrictions on External System Connections

The organization employs [*deny-all, permit-by-exception*] policy for allowing [*NRC information subsystems*] to connect to external information subsystems.

Supplemental Guidance: Organizations can constrain information subsystem connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as blacklisting (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as whitelisting (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7.

Control Enhancement 5 Implementation Detail	**Assessed Status:**	

CA-5 Plan of Action and Milestones

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. develops a plan of action and milestones for the information subsystem to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. updates existing plan of action and milestones [*at least quarterly*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB. Related controls: CA-2, CA-7, CM-4, PM-4.

Control Enhancements: None.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

Main Control Implementation Detail	**Assessed Status:**	

CA-6 Security Authorization

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. assigns a senior-level executive or manager as the authorizing official for the information subsystem;

b. ensures that the authorizing official authorizes the information subsystem for processing before commencing operations; and

c. updates the security authorization with the following frequency:[*(i) in accordance with DAA determined frequency for the system (e.g., at least every 3 years, on-going); (ii) when significant continuous monitoring issues exist; (iii) when significant security breaches occur; or (iv) when significant changes are made to the information subsystem or the environment in which the system operates*].

Supplemental Guidance: Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information subsystems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information subsystems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information subsystems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information subsystems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information subsystem owners with an up-to-date status of the security state of organizational information subsystems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10.

Control Enhancements: None.

References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publications 800-37, 800-137.

Main Control Implementation Detail	**Assessed Status:**	

CA-7 Continuous Monitoring

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**

Main Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. the establishment of the following metrics to be monitored and assessments supporting such monitoring:

- [*Perform a Security Control Test (ASCT) at least annually.*
- *Conduct vulnerability and configuration compliance scans of the system at least quarterly.*
- *Perform ad hoc scans on the system as needed to ensure security controls are operating as intended.*

- *Review and update system's security documents at least annually and when there is a significant change to the system (e.g., an approved configuration management changes made to the system).*
- *Review and update the system's plan of actions and milestones (POA&M) report at least quarterly and upon identification of a POA&M relevant finding.*
- *Test the system's contingency plan at least annually and when there is a significant change to the system.*
- *Review all security issues at least quarterly to ensure the system's security controls are operating as intended and have not degraded.*]

b. ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

c. ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

d. correlation and analysis of security-related information generated by assessments and monitoring;

e. response actions to address results of the analysis of security-related information; and

f. reporting the security status of organization and the information subsystem to [*CIO; CISO; DAA; CSO SITSO with responsibility for continuous monitoring oversight; Director, OIS; system ISSOs; system owners*];

Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information subsystems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information subsystems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

References: OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Continuous Monitoring | Independent Assessment

The organization employs assessors or assessment teams to monitor the security controls in the information subsystem on an ongoing basis with [*the required skills, experience, and technical expertise for conducting an impartial assessment of security controls employed within or inherited by the information subsystem*].

Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

CA-8 Penetration Testing

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**<Common>**

Main Control: The organization conducts penetration testing [*at least annually*] on [*the NRC infrastructure*].

Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on information subsystems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information subsystems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information subsystem and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

CA-9 Internal System Connections

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. authorizes internal connections of [*IT resources (e.g., servers, workstations, network devices, mobile devices, mobile workstations, wireless access points, network access storage devices (NAS), network printers, copiers, sensors, and scanners)*] to the information subsystem; and

b. documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Supplemental Guidance: This control applies to connections between organizational information subsystems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration. Related controls: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

CM-1 Configuration Management Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to the following personnel: [*CIO, CISO, DAA, IT executive, IT manager, IT functional manager, IT systems development official, IT auditor, system owners, ISSOs, office ISSOs, system administrators (e.g., database, network)*]: (i) a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. reviews and updates [*as needed*] the current: (i) configuration management policy [at least annually]; and (ii) configuration management procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

CM-2 Baseline Configuration

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information subsystem.

Supplemental Guidance: This control establishes baseline configurations for information subsystems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information subsystems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information subsystems. Baseline configurations include information about information subsystem components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information subsystems change over time. Baseline configurations of information subsystems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.

References: NIST Special Publication 800-128.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Baseline Configuration | Reviews and Updates

The organization reviews and updates the baseline configuration of the information subsystem:

a. [*at least annually*];

b. when required due to [*(i) any change to the system baseline configuration; (ii) any change to the system boundary; (iii) a change in the system's threat environment; (iv) In response to a significant security incident; or (v) any approved significant changes.*]; and

c. as an integral part of information subsystem component installations and upgrades.

Supplemental Guidance: Related control: CM-5.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Baseline Configuration | Automation Support for Accuracy / Currency

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information subsystem.

Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for information subsystems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information subsystem level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information subsystem component inventory and baseline configuration activities. Related controls: CM-7, RA-5.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 3: Baseline Configuration | Retention of Previous Configurations

The organization retains [*the most recent prior version of the baseline configuration for Low sensitivity systems and 2 previous versions of the baseline configuration for Moderate and High sensitivity systems*] to support rollback.

Supplemental Guidance: Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 7: Baseline Configuration | Configure systems, Components, or Devices for High-Risk Areas

The organization:

a. issues [*information technologies (e.g., devices) that are issued to NRC employees traveling to high risk areas are configured to the same configuration standards that would apply to a High sensitivity system with High confidentiality, integrity, and availability sensitivity. In addition, these devices shall be configured to reduce elevated risks to NRC property by employing full disk encryption, encrypting network communications, disabling any unnecessary hardware (e.g., wireless connectivity if it is not required), and applying all applicable NRC standards (e.g., for hardening)*]; and

b. applies [*security safeguards, such as wiping or re-imaging*] to the devices when the individuals return [*in accordance with CSO standards*].

Supplemental Guidance: When it is known that information subsystems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to

organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

Control Enhancement 7 Implementation Detail	**Assessed Status:**	

CM-3 Configuration Change Control

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. determines the types of changes to the information subsystem that are configuration-controlled;

b. reviews proposed configuration-controlled changes to the information subsystem and approves or disapproves such changes with explicit consideration for security impact analyses;

c. documents configuration change decisions associated with the information subsystem;

d. implements approved configuration-controlled changes to the information subsystem;

e. retains records of configuration-controlled changes to the information subsystem [*in accordance with MD 3.53 for unclassified systems*];

f. audits and reviews activities associated with configuration-controlled changes to the information subsystem; and

g. coordinates and provides oversight for configuration change control activities through [*governance boards (e.g., Change Control Board [CCB])*] that convenes [*at least quarterly and as needed for emergency changes*].

Supplemental Guidance: Configuration change controls for organizational information subsystems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information subsystems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information subsystems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information subsystems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information subsystems and the auditing activities required to implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

References: NIST Special Publication 800-128.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Configuration Change Control | Automated Document / Notification / Prohibition of Changes

The organization employs automated mechanisms to:

a. document proposed changes to the information subsystem;

b. notify [*the system's configuration management board (CMB)*] of proposed changes to the information subsystem and request change approval;

c. highlight proposed changes to the information subsystem that have not been approved or disapproved [*within at*

least 1 week];

d. prohibit changes to the information subsystem until designated approvals are received;

e. document all changes to the information subsystem; and

f. notify [*system owner, system ISSO, and system administrator*] when approved changes to the information subsystem are completed.

Supplemental Guidance: None.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Configuration Change Control | Test / Validate / Document Changes

The organization tests, validates, and documents changes to the information subsystem before implementing the changes on the operational system.

Supplemental Guidance: Changes to information subsystems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information subsystem operations. Individuals/groups conducting tests understand organizational security policies and procedures, information subsystem security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information subsystems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

CM-4 Security Impact Analysis

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.

Control Type:	**Hybrid**

Main Control: The organization analyzes changes to the information subsystem to determine potential security impacts prior to change implementation.

Supplemental Guidance: Organizational personnel with information security responsibilities (e.g., Information subsystem Administrators, Information subsystem Security Officers, Information subsystem Security Managers, and Information subsystem Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information subsystems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information subsystems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

References: NIST Special Publication 800-128.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Security Impact Analysis | Separate Test Environments

The organization analyzes changes to the information subsystem in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility,

or intentional malice. Supplemental Guidance: Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines). Related controls: SA-11, SC-3, SC-7.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

CM-5 Access Restrictions for Change

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information subsystem.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of information subsystems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information subsystems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information subsystems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Access Restrictions for Change | Automated Access Enforcement / Auditing

The information subsystem enforces access restrictions and supports auditing of the enforcement actions.

Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Access Restrictions for Change | Review System Changes

The organization reviews information subsystem changes [*at least quarterly, in accordance with continuous monitoring requirements*] and [*when indications so warrant*] to determine whether unauthorized changes have occurred.

Supplemental Guidance: Indications that warrant review of information subsystem changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. Related controls: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 3: Access Restrictions for Change | Signed Components

The information subsystem prevents the installation of [*device drivers, ActiveX components, macros, patches, hot fixes, operating system upgrades, application upgrades, and firmware (e.g., Uniform Extensible Firmware Interface [UEFI], Basic Input/Output System [BIOS] upgrades)*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication. Related controls: CM-7, SC-13, SI-7.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

CM-6 Configuration Settings

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. establishes and documents configuration settings for information technology products employed within the information subsystem using [*CSO standards and external standards located on the CSO web page*] that reflect the most restrictive mode consistent with operational requirements;

b. implements the configuration settings;

c. identifies, documents, and approves any deviations from established configuration settings for [*configurable information subsystem components*] based on [*deviations specified as in-scope with adequate justification and compensating controls per CSO-PROS-1324, "NRC Deviation Request Process"*]; and

d. monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information subsystem that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information subsystems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information subsystems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information subsystem components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol

(e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information subsystems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: http://nvd.nist.gov, http://checklists.nist.gov, http://www.nsa.gov.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Configuration Settings | Automated Central Management / Application / Verification

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*network-accessible hardware and software components of the information subsystem that affect the security posture and/or functionality of the system.*].

Supplemental Guidance: Related controls: CA-7, CM-4.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Configuration Settings | Respond to Unauthorized Changes

The organization employs [*automated or manual mechanisms in the form of an alert or the restoration of settings*] to respond to unauthorized changes to [*information subsystem configuration settings for network-accessible hardware and software components of the information subsystem that affect the security posture and/or functionality of the system*].

Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information subsystem processing. Related controls: IR-4, SI-7.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

CM-7 Least Functionality

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.

Control Type:	**System-Specific**

Main Control: The organization:

a. configures the information subsystem to provide only essential capabilities; and

b. prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*in accordance with CSO-STD-2008, "Network Protocol Standard."*].

Supplemental Guidance: Information subsystems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information subsystem components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information subsystems or individual components of information subsystems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing).

Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information subsystems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and

services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7. References: DoD Instruction 8551.01.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Least Functionality | Periodic Review The organization: a. reviews the information subsystem [*at least annually*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and b. disables [*unnecessary and/or nonsecure functions, ports, protocols, and services as well as ensure the information subsystem adheres to requirements specified in CSO-STD-2008.*]. Supplemental Guidance: The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Least Functionality | Prevent Program Execution The information subsystem prevents program execution in accordance with [*rules authorizing the terms and conditions of software program usage and the list of software programs authorized to execute on the information subsystem (e.g., application whitelisting).*]. Supplemental Guidance: Related controls: CM-8, PM-5.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 5: Least Functionality | Authorized Software / Whitelisting The organization: a. develops and maintains [*a list of software programs authorized to execute on the information subsystem.*]; b. employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information subsystem; and c. reviews and updates the list of authorized software programs [*at least annually.*]. Supplemental Guidance: The process used to identify software programs that are authorized to execute on organizational information subsystems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.		
Control Enhancement 5 Implementation Detail	**Assessed Status:**	

CM-8 Information subsystem Component Inventory

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**
Main Control: The organization:		

a. develops and documents an inventory of information subsystem components that: (i) accurately reflects the current information subsystem; (ii) Includes all components within the authorization boundary of the information subsystem; (iii) is at the level of granularity deemed necessary for tracking and reporting; and (iv) includes:

- [*System Name*
- *Asset Role (e.g., Windows Domain Controller vs. Windows Member Server; Perimeter Switch vs. Infrastructure Switch)*
- *Asset Type (e.g., firewall, server, workstation)*
- *Virtual or Physical Device*
- *Virtual Machine/Instance Host (server or cluster)*
- *Manufacturer*
- *Manufacturer Model Number/Version*
- *Manufacturer Serial Number*
- *Asset Tag (if owned/leased by the NRC)*
- *Unique Host Name (if available the host's fully qualified domain name should be used)*
- *Location (i.e., site, building, and room where the asset is located)*
- *Operating System Name*
- *Operating System Version*
- *Licensing Information*
- *License Expiration Date*]; and

b. reviews and updates the information subsystem component inventory [*at least annually and within 30 days of hardware or software changes within the system.*].

Supplemental Guidance: Organizations may choose to implement centralized information subsystem component inventories that include components from all organizational information subsystems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information subsystem association, information subsystem owner). Information deemed necessary for effective accountability of information subsystem components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5.

References: NIST Special Publication 800-128.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Information subsystem Component Inventory | Updates During Installations / Removals

The organization updates the inventory of information subsystem components as an integral part of component installations, removals, and information subsystem updates.

Supplemental Guidance: None.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Information subsystem Component Inventory | Automated Maintenance

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information subsystem components.

Supplemental Guidance: Organizations maintain information subsystem inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine information subsystem component inventory and baseline configuration activities. Related

control: SI-7.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	

Control Enhancement 3: Information subsystem Component Inventory | Automated Unauthorized Component Detection

The organization:

a. employs automated mechanisms [*continuously*] to detect the presence of unauthorized hardware, software, and firmware components within the information subsystem; and

b. takes the following actions when unauthorized components are detected:

- [*Notify the system ISSO and administrators, and*
- *Perform any other actions required in accordance with CSO-STD-0021.*].

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information subsystems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information subsystem components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing. Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	

Control Enhancement 4: Information subsystem Component Inventory | Accountability Information

The organization includes in the information subsystem component inventory information, a means for identifying [*by name, position, and role (e.g., cybersecurity roles based on the NRC Cybersecurity Workforce Development Plan)*], individuals responsible/accountable for administering those components.

Supplemental Guidance: Identifying individuals who are both responsible and accountable for administering information subsystem components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required (e.g., component is determined to be the source of a breach/compromise, component needs to be recalled/replaced, or component needs to be relocated).

Control Enhancement 4 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	

Control Enhancement 5: Information subsystem Component Inventory | No Duplicate Accounting of Components

The organization verifies that all components within the authorization boundary of the information subsystem are not duplicated in other information subsystem inventories.

Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information subsystem components in large or complex interconnected systems.

Control Enhancement 5 Implementation Detail	**Assessed Status:**	

CM-9 Configuration Management Plan

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization develops, documents, and implements a configuration management plan for the information subsystem that:

a. addresses roles, responsibilities, and configuration management processes and procedures;

b. establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. defines the configuration items for the information subsystem and places the configuration items under configuration management; and

d. protects the configuration management plan from unauthorized disclosure and modification.

Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information subsystems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information subsystem level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information subsystem component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information subsystems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information subsystem items (hardware, software, firmware, and documentation) to be configuration-managed. As information subsystems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.

Control Enhancements: None.

References: NIST Special Publication 800-128.

Main Control Implementation Detail	**Assessed Status:**	

CM-10 Software Usage Restrictions

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. uses software and associated documentation in accordance with contract agreements and copyright laws;

b. tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7.

Control Enhancements: None.

References: None.		
Main Control Implementation Detail	**Assessed Status:**	

CM-11 User-Installed Software

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. governs the installation of software by users in accordance with [*the NRC MDs and the "NRC Agency-wide Rules of Behavior for Authorized Computer Use"*];

b. enforces software installation policies through [*automated mechanisms*]; and

c. monitors policy compliance [*continuously in accordance with NRC MDs and the "NRC Agency-wide Rules of Behavior for Authorized Computer Use" regarding user installed authorized and unauthorized software on information subsystems using NRC automated security applications, in accordance with CSO-PROS-1323, "U.S. Nuclear Regulatory Commission Agency-wide Continuous Monitoring Program."*]

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational information subsystems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information subsystems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

CP-1 Contingency Planning Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*Chief Information Officer (CIO); Chief Information Security Officer (CISO); Designated Approving Authority (DAA); information technology (IT) executive; IT manager; IT functional manager; IT systems development official; IT auditors; system owners; system information subsystem security officer (ISSO); system administrators (database, network, etc.)*]: (i) a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

b. reviews and updates [*as needed*] the current: (i) contingency planning policy [*at least annually*]; and (ii) contingency planning procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security

program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

CP-2 Contingency Plan

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. develops a contingency plan for the information subsystem that: (i) identifies essential missions and business functions and associated contingency requirements; (ii) provides recovery objectives, restoration priorities, and metrics; (iii) addresses contingency roles, responsibilities, assigned individuals with contact information; (iv) addresses maintaining essential missions and business functions despite an information subsystem disruption, compromise, or failure; (v) addresses eventual, full information subsystem restoration without deterioration of the security safeguards originally planned and implemented; and (vi) is reviewed and approved by the [*DAA*];

b. distributes copies of the contingency plan to [*Director, Office of Information Services (OIS) via the OIS Regulatory Information Distribution System (RIDS) email address; CISO via the CSO RIDS email address; system owners; system ISSO*];

c. coordinates contingency planning activities with incident handling activities;

d. reviews the contingency plan for the information subsystem [*at least annually*];

e. updates the contingency plan to address changes to the organization, information subsystem, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. communicates contingency plan changes to [*Director, OIS via the OIS RIDS email address; CISO via the CSO RIDS email address; system owners; and system ISSO*]; and

g. protects the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: Contingency planning for information subsystems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information subsystem restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information subsystem resiliency. Contingency plans reflect the degree of restoration required for organizational information subsystems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information subsystem recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information subsystem availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information subsystems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information subsystem shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Contingency Plan | Coordinate with Related Plans The organization coordinates contingency plan development with organizational elements responsible for related plans. Supplemental Guidance: Plans related to contingency plans for organizational information subsystems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Contingency Plan | Capacity Planning The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. Supplemental Guidance: Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber-attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 3: Contingency Plan | Resume Essential Missions / Business Functions The organization plans for the resumption of essential mission and business functions within the following timeframes: [*(i) 14 system business days (moderate availability sensitivity)*; (ii) *3 system business days (high availability sensitivity)*; or (iii) the *business impact assessment (BIA) timeframe if shorter duration*] of contingency plan activation. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information subsystem and its supporting infrastructure. Related control: PE-12.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 4: Contingency Plan | Resume All Missions / Business Functions The organization plans for the resumption of all missions and business functions within [*within 3 system business days (high availability sensitivity)*] of contingency plan activation. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information subsystem and its supporting infrastructure. Related control: PE-12.		
Control Enhancement 4 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 5: Contingency Plan | Continue Essential Missions / Business Functions		

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information subsystem restoration at primary processing and/or storage sites. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.		
Control Enhancement 5 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 8: Contingency Plan | Identify Critical Assets The organization identifies critical information subsystem assets supporting essential missions and business functions. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information subsystem assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information subsystem assets include technical and operational aspects. Technical aspects include, for example, information technology services, information subsystem components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. Related controls: SA-14, SA-15.		
Control Enhancement 8 Implementation Detail	**Assessed Status:**	

CP-3 Contingency Training

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:	**System-Specific**	
Main Control: The organization provides contingency training to information subsystem users consistent with assigned roles and responsibilities: a. within [*30 days of assuming a contingency role and responsibility and when required by information subsystem changes*]; b. when required by information subsystem changes; and c. [*at least annually*] thereafter. Supplemental Guidance: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information subsystems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, CP-2, IR-2. References: Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50.		

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**
Control Enhancement 1: Contingency Training | Simulated Events The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations. Supplemental Guidance: None.	

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

CP-4 Contingency Plan Testing

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. tests the contingency plan for the information subsystem to determine the effectiveness of the plan and the organizational readiness to execute the plan:

- [*at least annually using a table-top test or functional exercise for systems with a low availability sensitivity*];
- [*at least annually using a table-top test or functional exercise and an actual test including the following at least every 3 years for systems with a moderate availability sensitivity*:
  - *system recovery on an alternate platform from backup media or a hot site*
  - *coordination among recovery teams*
  - *internal and external connectivity*
  - *comparable system performance using alternate equipment*
  - *restoration of normal operations*
  - *notification procedures*];
- [*at least annually using an actual test including the following for systems with a high availability sensitivity and at least every 3 years at the alternate processing site*:
  - *system recovery on an alternate platform from backup media or a hot site*
  - *coordination among recovery teams*
  - *internal and external connectivity*
  - *comparable system performance using alternate equipment*
  - *restoration of normal operations*
  - *notification procedures*];

b. reviews the contingency plan test results; and

c. initiates corrective actions, if needed.

Supplemental Guidance: Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3.

References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Contingency Plan Testing | Coordinate with Related Plans

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information subsystems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related controls: IR-8, PM-8.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Contingency Plan Testing | Alternate Processing Site

The organization tests the contingency plan at the alternate processing site:

a. to familiarize contingency personnel with the facility and available resources; and

b. to evaluate the capabilities of the alternate processing site to support contingency operations.

Supplemental Guidance: Related control: CP-7.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

CP-6 Alternate Storage Site

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.

Control Type:	**System-Specific**

Main Control: The organization:

a. establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information subsystem backup information; and

b. ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information subsystems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.

References: NIST Special Publication 800-34.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Alternate Storage Site | Separation from Primary Site

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant. Related control: RA-3.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Alternate Storage Site | Recovery Time / Point Objectives The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. Supplemental Guidance: None.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 3: Alternate Storage Site | Accessibility 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. Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	

CP-7 Alternate Processing Site

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**System-Specific**	
Main Control: The organization: a. establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*information subsystem operations*] for essential missions/business functions within [*(i) 14 system business days (moderate availability sensitivity); or (ii) 3 system business days (high availability sensitivity)*] when the primary processing capabilities are unavailable; b. ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site. Supplemental Guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information subsystems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10,		

MA-6. References: NIST Special Publication 800-34.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Alternate Processing Site | Separation from Primary Site The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats. Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant. Related control: RA-3.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Alternate Processing Site | Accessibility 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. Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Related control: RA-3.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 3: Alternate Processing Site | Priority of Service The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives). Supplemental Guidance: Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 4: Alternate Processing Site | Preparation for Use The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions. Supplemental Guidance: Site preparation includes, for example, establishing configuration settings for information subsystem components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place. Related controls: CM-2, CM-6.		
Control Enhancement 4 Implementation Detail	**Assessed Status:**	

CP-8 Telecommunications Services

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*information subsystem operations*] for essential missions and business functions within [*(i) 14 system business days (moderate availability sensitivity); or (ii) 3 system business days (high availability sensitivity)*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Supplemental Guidance: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits / lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7.

References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: http://www.dhs.gov/telecommunications-service-priority-tsp.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Telecommunications Services | Priority of Service Provisions

The organization:

a. develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

b. requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Supplemental Guidance: Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 2: Telecommunications Services | Single Points of Failure

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Supplemental Guidance: None.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 3: Telecommunications Services | Separation of Primary / Alternate Providers

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation

between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 4: Telecommunications Services | Provider Contingency Plan The organization: a. requires primary and alternate telecommunications service providers to have contingency plans; b. reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and c. obtains evidence of contingency testing/training by providers in accordance with [*Management Directive (MD) 12.4, "NRC Telecommunications Systems Security Program"*]. Supplemental Guidance: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.		
Control Enhancement 4 Implementation Detail	**Assessed Status:**	

CP-9 Information subsystem Backup

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**System-Specific**	
Main Control: The organization: a. conducts backups of user-level information contained in the information subsystem [*in accordance with CSO-STD-2002, "System Back-up Standard."*]; b. conducts backups of system-level information contained in the information subsystem [*in accordance with CSO-STD-2002, "System Back-up Standard."*]; c. conducts backups of information subsystem documentation including security-related documentation [*in accordance with CSO-STD-2002, "System Back-up Standard."*]; and d. protects the confidentiality, integrity, and availability of backup information at storage locations. Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information subsystem backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information subsystem backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13. References: NIST Special Publication 800-34.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Information subsystem Backup | Testing For Reliability / Integrity The organization tests backup information [*at least annually*] to verify media reliability and information integrity.		

Supplemental Guidance: Related control: CP-4.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Information subsystem Backup | Test Restoration Using Sampling The organization uses a sample of backup information in the restoration of selected information subsystem functions as part of contingency plan testing. Supplemental Guidance: Related control: CP-4.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 3: Information subsystem Backup | Separate Storage For Critical Information The organization stores backup copies of [*critical information subsystem software (e.g., operating systems, cryptographic key management systems, and intrusion detection/prevention systems) and other security-related information (e.g., organizational inventories of hardware, software, and firmware components), as identified from the system BIA and Business Area Risk Assessment (BARA)*] in a separate facility or in a fire-rated container that is not collocated with the operational system. Supplemental Guidance: Critical information subsystem software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations. Related controls: CM-2, CM-8.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 5: Information subsystem Backup | Transfer To Alternate Storage Site The organization transfers information subsystem backup information to the alternate storage site [*in accordance with CSO-STD-2002, "System Back-up Standard."*]. Supplemental Guidance: Information subsystem backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.		
Control Enhancement 5 Implementation Detail	**Assessed Status:**	

CP-10 Information subsystem Recovery and Reconstitution

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**
Main Control: The organization provides for the recovery and reconstitution of the information subsystem to a known state after a disruption, compromise, or failure. Supplemental Guidance: Recovery is executing information subsystem contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information subsystems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information subsystem capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information subsystem capabilities, reestablishment of continuous monitoring activities, potential information subsystem reauthorizations, and activities to prepare the systems against		

future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24. References: Federal Continuity Directive 1; NIST Special Publication 800-34.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Information subsystem Recovery And Reconstitution | Transaction Recovery The information subsystem implements transaction recovery for systems that are transaction-based. Supplemental Guidance: Transaction-based information subsystems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 4: Information subsystem Recovery And Reconstitution | Restore Within Time Period The organization provides the capability to restore information subsystem components within [*24 hours*] from configuration-controlled and integrity-protected information representing a known, operational state for the components. Supplemental Guidance: Restoration of information subsystem components includes, for example, reimaging which restores components to known, operational states. Related control: CM-2.		
Control Enhancement 4 Implementation Detail	**Assessed Status:**	

DI-1 Data Quality

Implementation Priority:	N/A	N/A
Control Type:	**System-Specific**	
Main Control: The organization: a. confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. collects PII directly from the individual to the greatest extent practicable; c. checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [*at least annually*]; and d. issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. Supplemental Guidance: Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information subsystems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals. When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information subsystems and develop corresponding procedures for how frequently, and by what method, the information is to be updated. Related controls: AP-2, DI-2, DM-1, IP-3, SI-10.		

References: The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB Memorandum 07-16.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Data Quality | Validate PII The organization requests that the individual or individual's authorized representative validate PII during the collection process. Supplemental Guidance: None.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Data Quality | Re-Validate PII The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate [*at least every 2 years*]. Supplemental Guidance: None.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	

DI-2 Data Integrity and Data Integrity Board

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**
Main Control: The organization: a. documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. Supplemental Guidance: Organizations conducting or participating in Computer Matching Agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO). The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under Computer Matching Agreements. Related controls: AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2. References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I.		
Main Control Implementation Detail		**Assessed Status:**
Control Type:		**<Common>**
Control Enhancement 1: Data Integrity and Data Integrity Board | Publish Agreements on Website The organization publishes Computer Matching Agreements on its public website. Supplemental Guidance: None.		

Control Enhancement 1 Implementation Detail	Assessed Status:	

DM-1 Minimization of Personally Identifiable Information

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

c. conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [*at least every 2 years*] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Supplemental Guidance: Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel to identify the minimum PII elements required by the information subsystem or activity to accomplish the legally authorized purpose.

Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules.

By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice. Related controls: AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1.

References: The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.

Main Control Implementation Detail	Assessed Status:	

Control Type:	System-Specific

Control Enhancement 1: Minimization of Personally Identifiable Information | Locate / Remove / Redact / Anonymize PII

The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

Supplemental Guidance: NIST Special Publication 800-122 provides guidance on anonymization.

Control Enhancement 1 Implementation Detail	Assessed Status:	

DM-2 Data Retention and Disposal

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. retains each collection of personally identifiable information (PII) for [*a period of up to 6 years*] to fulfill the purpose(s) identified in the notice or as required by law;

b. disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. uses [*media sanitization techniques and procedures defined in CSO-STD-2004*] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Supplemental Guidance: NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.

Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII.

Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB Memorandum 07-16; OMB Circular A-130; NIST Special Publication 800-88.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Data Retention and Disposal | System Configuration

The organization, where feasible, configures its information subsystems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

Supplemental Guidance: None.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

DM-3 Minimization of PII Used in Testing, Training, and Research

Implementation Priority:	N/A	N/A
Control Type:		**System-Specific**

Main Control: The organization:

a. develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and

b. implements controls to protect PII used for testing, training, and research.

Supplemental Guidance: Organizations often use PII for testing new applications or information subsystems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations

take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the SAOP/CPO and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected. References: NIST Special Publication 800-122.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Minimization of PII Used in Testing, Training, and Research | Risk Minimization Techniques The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training. Supplemental Guidance: Organizations can minimize risk to privacy of PII by using techniques such as de-identification.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

IA-1 Identification and Authentication Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**Hybrid**	

Main Control: The organization:

a. develops, documents, and disseminates to the [*Chief Information Officer (CIO), Chief Information Security Officer (CISO), Designated Approving Authority (DAA), Computer Security Office (CSO) Senior Information Technology Officer (SITSO) with responsibility for continuous monitoring oversight, Director, Office of Information Services (OIS), system information subsystem security officer (ISSO), system owners*]: (i) an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. reviews and updates [*as needed*] the current: (i) identification and authentication policy [*at least annually*]; and (ii) identification and authentication procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

IA-2 Identification and Authentication (Organizational Users)

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The information subsystem uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information subsystems is defined as either local access or network access. Local access is any access to organizational information subsystems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information subsystems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information subsystems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information subsystem level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Identification And Authentication | Network Access To Privileged Accounts

The information subsystem implements multifactor authentication for network access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Identification And Authentication | Network Access To Non-Privileged Accounts

The information subsystem implements multifactor authentication for network access to non-privileged accounts.

Supplemental Guidance: None.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 3: Identification And Authentication | Local Access To Privileged Accounts

The information subsystem implements multifactor authentication for local access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 4: Identification And Authentication | Local Access To Non-Privileged Accounts

The information subsystem implements multifactor authentication for local access to non-privileged accounts.

Supplemental Guidance: None.

Control Enhancement 4 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 8: Identification And Authentication | Network Access To Privileged Accounts - Replay Resistant

The information subsystem implements replay-resistant authentication mechanisms for network access to privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

Control Enhancement 8 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 9: Identification And Authentication | Network Access To Non-Privileged Accounts - Replay Resistant

The information subsystem implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

Control Enhancement 9 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 11: Identification And Authentication | Remote Access - Separate Device

The information subsystem implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*requirements for logical and physical access defined in Federal Information Processing Standard (FIPS) 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors"*].

Supplemental Guidance: For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information subsystem gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example,

adversaries deploying malicious code on organizational information subsystems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. Related control: AC-6.		
Control Enhancement 11 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 12: Identification And Authentication | Acceptance Of PIV Credentials The information subsystem accepts and electronically verifies Personal Identity Verification (PIV) credentials. Supplemental Guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.		
Control Enhancement 12 Implementation Detail	**Assessed Status:**	

IA-3 Device Identification and Authentication

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**System-Specific**	
Main Control: The information subsystem uniquely identifies and authenticates [*workstations (desktops and laptops), servers, firewalls, routers, switches, mobile devices, security devices/appliances, wireless devices/appliances*] before establishing a connection. Supplemental Guidance: Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information subsystems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information subsystems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5. Control Enhancements: None. References: None.		
Main Control Implementation Detail	**Assessed Status:**	

IA-4 Identifier Management

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**Hybrid**	
Main Control: The organization manages information subsystem identifiers by: a. receiving authorization from [*the system owner*] to assign an individual, group, role, or device identifier; b. selecting an identifier that identifies an individual, group, role, or device; c. assigning the identifier to the intended individual, group, role, or device;		

d. preventing reuse of identifiers for [*at least 5 years*]; and

e. disabling the identifier after [*no more than 35 days of inactivity*].

Supplemental Guidance: Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information subsystem accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information subsystem accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information subsystem accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information subsystems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

Main Control Implementation Detail	**Assessed Status:**	

IA-5 Authenticator Management

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization manages information subsystem authenticators by:

a. verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. establishing initial authenticator content for authenticators defined by the organization;

c. ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

e. changing default content of authenticators prior to information subsystem installation;

f. establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. changing/refreshing authenticators [*(i) at least every 5 years for PIV cards and other hard tokens; (ii) at least every 3 years for PIV authentication certificate; (iii) at least every 3 years for soft digital certificates; and (vi) in accordance with CSO-STD-0001, "NRC Strong Password Standard" for passwords*];

h. protecting authenticator content from unauthorized disclosure and modification;

i. requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

j. changing authenticators for group/role accounts when membership to those accounts changes.

Supplemental Guidance: Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information subsystem components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information subsystems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information subsystems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when

no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Authenticator Management | Password-Based Authentication

The information subsystem, for password-based authentication:

a. Enforces minimum password complexity that [*is in accordance with CSO-STD-0001, "NRC Strong Password Standard."*];

b. Ensures the requirements for changed characters when new passwords are created: [*are in accordance with CSO-STD-0001, "NRC Strong Password Standard."*];

c. Stores and transmits only encrypted representations of passwords;

d. Ensures password minimum and maximum lifetime restrictions are [*in accordance with CSO-STD-0001, "NRC Strong Password Standard."*];

e. Ensures password reuse requirements are [*in accordance with CSO-STD-0001, "NRC Strong Password Standard."*] generations; and

f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Supplemental Guidance: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. Related control: IA-6.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 2: Authenticator Management | PKI-Based Authentication

The information subsystem, for PKI-based authentication:

a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

b. Enforces authorized access to the corresponding private key;

c. Maps the authenticated identity to the account of the individual or group; and

d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing. Related control: IA-6.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 3: Authenticator Management | In-Person Or Trusted Third-Party Registration

The organization requires that the registration process to receive [*initial issuance of digital certificates and hard*

tokens for level 4 authentication] be conducted [*in person*] before [*a designated registration authority*].] Supplemental Guidance: None.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**
Control Enhancement 11: Authenticator Management | Hardware Token-Based Authentication The information subsystem, for hardware token-based authentication, employs mechanisms that satisfy [*token quality requirements defined in FIPS 201-1, "PIV of Federal Employees and Contractors."*]. Supplemental Guidance: Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.	

Control Enhancement 11 Implementation Detail	**Assessed Status:**	

IA-6 Authenticator Feedback

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**
Main Control: The information subsystem obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. Supplemental Guidance: The feedback from information subsystems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information subsystems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. Related control: PE-18. Control Enhancements: None. References: None.		

Main Control Implementation Detail	**Assessed Status:**	

IA-7 Cryptographic Module Authentication

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**
Main Control: The information subsystem implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. Supplemental Guidance: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Related controls: SC-12, SC-13.		

Control Enhancements: None. References: FIPS Publication 140; Web: http://csrc.nist.gov/groups/STM/cmvp/index.html.		
Main Control Implementation Detail	**Assessed Status:**	

IA-8 Identification and Authentication (Non-Organizational Users)

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance: Non-organizational users include information subsystem users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information subsystems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information subsystems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information subsystems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.

References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: http://idmanagement.gov.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Identification And Authentication | Acceptance Of PIV Credentials From Other Agencies

The information subsystem accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Identification and Authentication | Acceptance Of Third-Party Credentials

The information subsystem accepts only FICAM-approved third-party credentials.

Supplemental Guidance: This control enhancement typically applies to organizational information subsystems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels. Related control: AU-2.

Control Enhancement 2 Implementation Detail	Assessed Status:	

Control Type:	System-Specific

Control Enhancement 3: Identification and Authentication | Use Of FICAM-Approved Products

The system owner employs only FICAM-approved information subsystem components in [*NRC systems that are accessible to the general public*] to accept third-party credentials.

Supplemental Guidance: This control enhancement typically applies to information subsystems that are accessible to the general public, for example, public-facing websites. FICAM-approved information subsystem components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. Related control: SA-4.

Control Enhancement 3 Implementation Detail	Assessed Status:	

Control Type:	System-Specific

Control Enhancement 4: Identification and Authentication | Use Of FICAM-Issued Profiles

The information subsystem conforms to FICAM-issued profiles.

Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). Related control: SA-4.

Control Enhancement 4 Implementation Detail	Assessed Status:	

IP-1 Consent

Implementation Priority:	N/A	N/A
Control Type:		**System-Specific**

Main Control: The organization:

a. provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;

b. provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

c. obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

d. ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Supplemental Guidance: Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.

Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. For example, the Federal Trade Commission's Do-Not-Call Registry allows individuals to

opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information subsystem, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization. Related controls: AC-2, AP-1, TR-1, TR-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-22.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**
Control Enhancement 1: Consent | Mechanisms Supporting Itemized or Tiered Consent The organization implements mechanisms to support itemized or tiered consent for specific uses of data. Supplemental Guidance: Organizations can provide, for example, individuals' itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that organizational operations comply with individual choices.	

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

IP-2 Individual Access

Implementation Priority:	N/A	N/A
Control Type:		
Control Type:		**Hybrid**

Main Control: The organization:

a. provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;

b. publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;

c. publishes access procedures in System of Records Notices (SORNs); and

d. adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Supplemental Guidance: Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding. Related controls: AR-8, IP-3, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4); (j), (k), (t); OMB Circular A-130.

Main Control Implementation Detail	**Assessed Status:**	

IP-3 Redress

Implementation Priority:	N/A	N/A
Control Type:		**System-Specific**

Main Control: The organization:

a. provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and

b. establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Supplemental Guidance: Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.

To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130.

Main Control Implementation Detail	**Assessed Status:**	

IP-4 Complaint Management

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control:

The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Supplemental Guidance: Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner. Related controls: AR-6, IP-3.

References: OMB Circular A-130; OMB Memoranda 07-16, 08-09.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Complaint Management | Response Times

The organization responds to complaints, concerns, or questions from individuals within [*5 business days*].

Supplemental Guidance: Organizations can provide, for example, individuals' itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that organizational operations comply with individual choices.

Control Enhancement 1 Implementation Detail	Assessed Status:	

IR-1 Incident Response Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*Chief Information Security Officer (CISO); Senior Information Technology Security Officer (SITSO), CSO/Cyber Situational Awareness, Analysis, and Response (CSAAR) Team; Director, Office of Information Services (OIS); Branch Chief, Office of Administration (ADM)/Division of Facilities Security (DFS)/Facilities Security Branch (FSB); system owners; system information subsystem security officer (ISSO); Computer Security Incident Response Team (CSIRT)*]: (i) an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. reviews and updates [*as needed*] the current: (i) incident response policy [*at least annually*]; and (ii) incident response procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

Main Control Implementation Detail	Assessed Status:	

IR-2 Incident Response Training

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**

Main Control: The organization provides incident response training to information subsystem users consistent with assigned roles and responsibilities:

a. within [*30 days*] of assuming an incident response role or responsibility;

b. when required by information subsystem changes; and

c. [*at least annually*] thereafter.

Supplemental Guidance: Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information subsystem; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from

external and internal sources. Related controls: AT-3, CP-3, IR-8. References: NIST Special Publications 800-16, 800-50.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 1: Incident Response Training | Simulated Events The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. Supplemental Guidance: None.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 2: Incident Response Training | Automated Training Environments The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment. Supplemental Guidance: None.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	

IR-3 Incident Response Testing

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:	**Hybrid**	
Main Control: The organization tests the incident response capability for the information subsystem to determine the incident response effectiveness and documents the results: - [*At least annually, using a table-top test or functional exercise (i.e., an exercise that allows personnel to validate their operational readiness by performing their duties in a simulated environment) for Low sensitivity systems.*]; - [*At least annually, using a table-top test or functional exercise and at least once every 3 years using an actual test for Moderate sensitivity systems.*]; - [*At least annually, using an actual test for High sensitivity systems.*] Supplemental Guidance: Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. Related controls: CP-4, IR-8. References: NIST Special Publications 800-84, 800-115.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 2: Incident Response Testing | Coordination With Related Plans The organization coordinates incident response testing with organizational elements responsible for related plans.		

Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	

IR-4 Incident Handling

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. coordinates incident handling activities with contingency planning activities; and

c. incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information subsystems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information subsystems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information subsystem owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

References: Executive Order 13587; NIST Special Publication 800-61.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Incident Handling | Automated Incident Handling Processes

The organization employs automated mechanisms to support the incident handling process.

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 4: Incident Handling | Information Correlation

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile cyber-attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.

Control Enhancement 4 Implementation Detail	**Assessed Status:**	

IR-5 Incident Monitoring

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization tracks and documents information subsystem security incidents.

Supplemental Guidance: Documenting information subsystem security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

References: NIST Special Publication 800-61.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Incident Monitoring | Automated Tracking / Data Collection / Analysis

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-7, IR-4.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

IR-6 Incident Reporting

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. requires personnel to report suspected security incidents to the organizational incident response capability [*within 1 hour of identifying a suspected incident.*]; and

b. reports security incident information to [*NRC CSIRT*].

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8.

References: NIST Special Publication 800-61: Web: http://www.us-cert.gov.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**<Common>**

Control Enhancement 1: Incident Reporting | Automated Reporting

The organization employs automated mechanisms to assist in the reporting of security incidents. Supplemental Guidance: Related control: IR-7.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

IR-7 Incident Response Assistance

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**<Common>**

Main Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information subsystem for the handling and reporting of security incidents.

Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**<Common>**

Control Enhancement 1: Incident Response Assistance | Automation Support For Availability Of Information / Support

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

IR-8 Incident Response Plan

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops an incident response plan that: (i) provides the organization with a roadmap for implementing its incident response capability; (ii) describes the structure and organization of the incident response capability; (iii) provides a high-level approach for how the incident response capability fits into the overall organization; (iv) meets the unique requirements of the organization, which relate to mission, size, structure, and functions; (v) defines reportable incidents; (vi) provides metrics for measuring the incident response capability within the organization; (vi) defines the resources and management support needed to effectively maintain and mature an incident response capability; and (vii) is reviewed and approved by [*Designated Approving Authority (DAA) for non-major IT investments*];

b. distributes copies of the incident response plan to [*DAA for non-major IT investments; Director, OIS/Operations*

Division; CSIRT; system ISSO; and system owners];

c. reviews the incident response plan [*at least annually*];

d. updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e. communicates incident response plan changes to [*DAA for non-major IT investments; Director, OIS/Operations Division; CSIRT; system ISSO; system owners*]; and

f. protects the incident response plan from unauthorized disclosure and modification.

Supplemental Guidance: It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information subsystems. Related controls: MP-2, MP-4, MP-5.

Control Enhancements: None.

References: NIST Special Publication 800-61.

Main Control Implementation Detail	**Assessed Status:**	

MA-1 System Maintenance Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [the *Chief Information Officer (CIO); Chief Information Security Officer (CISO); Designated Approving Authority (DAA); Director, Office of Information Services (OIS); system information subsystem security officers (ISSOs); system owners*]: (i) a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. reviews and updates [*as needed*] the current: (i) system maintenance policy [*at least annually*]; and (ii) system maintenance procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

MA-2 Controlled Maintenance

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. schedules, performs, documents, and reviews records of maintenance and repairs on information subsystem components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. requires that [*the property custodian*] explicitly approve the removal of the information subsystem or system components from organizational facilities for off-site maintenance or repairs;

d. sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

e. checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. includes the following information in maintenance records: [*(i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) description of the maintenance performed; and (v) information subsystem components/equipment removed or replaced (including identification numbers, if applicable)*].

Supplemental Guidance: This control addresses the information security aspects of the information subsystem maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information subsystem components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information subsystems. Organizations consider supply chain issues associated with replacement components for information subsystems. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Controlled Maintenance | Automated Maintenance Activities

The organization:

a. employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and

b. produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

Supplemental Guidance: Related controls: CA-7, MA-3.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

MA-3 Maintenance Tools

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.

Control Type:	**System-Specific**

Main Control: The organization approves, controls, and monitors information subsystem maintenance tools.

Supplemental Guidance: This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information subsystems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information subsystems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information subsystem maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6.

References: NIST Special Publication 800-88.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Maintenance Tools | Inspect Tools

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling. Related control: SI-7.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Maintenance Tools | Inspect Media

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information subsystem.

Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures. Related control: SI-3.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 3: Maintenance Tools | Prevent Unauthorized Removal

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

a. verifying that there is no organizational information contained on the equipment;

b. sanitizing or destroying the equipment;

c. retaining the equipment within the facility; or

d. obtaining an exemption from [*the property custodian*] explicitly authorizing removal of the equipment from the facility.

Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

Control Enhancement 3 Implementation Detail	Assessed Status:	

MA-4 Nonlocal Maintenance

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.

Control Type:	System-Specific

Main Control: The organization:

a. approves and monitors nonlocal maintenance and diagnostic activities;

b. allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information subsystem;

c. employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. maintains records for nonlocal maintenance and diagnostic activities; and

e. terminates session and network connections when nonlocal maintenance is completed.

Supplemental Guidance: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information subsystem or information subsystem component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

Main Control Implementation Detail	Assessed Status:	

Control Type:	System-Specific

Control Enhancement 2: Nonlocal Maintenance | Document Nonlocal Maintenance

The organization documents in the security plan for the information subsystem, the policies, and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

Supplemental Guidance: None.

Control Enhancement 2 Implementation Detail	Assessed Status:	

Control Type:	System-Specific

Control Enhancement 3: Nonlocal Maintenance | Comparable Security / Sanitization

The organization:

a. requires that nonlocal maintenance and diagnostic services be performed from an information subsystem that implements a security capability comparable to the capability implemented on the system being serviced; or

b. removes the component to be serviced from the information subsystem and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information subsystem.

Supplemental Guidance: Comparable security capability on information subsystems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information subsystem being serviced. Related

controls: MA-3, SA-12, SI-3, SI-7.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	

MA-5 Maintenance Personnel

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

b. ensures that non-escorted personnel performing maintenance on the information subsystem have required access authorizations; and

c. designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Supplemental Guidance: This control applies to individuals performing hardware or software maintenance on organizational information subsystems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information subsystems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information subsystems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods. Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Maintenance Personnel | Individuals Without Appropriate Access

The organization:

a. implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: (i) maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information subsystem by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; (ii) prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information subsystem are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

b. develops and implements alternate security safeguards in the event an information subsystem component cannot be sanitized, removed, or disconnected from the system.

Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information subsystems. Procedures for the use of maintenance personnel can be documented in security plans for the information subsystems. Related controls: MP-6, PL-2.

Control Enhancement 1 Implementation Detail	Assessed Status:	

MA-6 Timely Maintenance

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization obtains maintenance support and/or spare parts for [*key components identified in the Business Impact Assessment (BIA)*] within [*(i) 14 business days of failure for systems with a Moderate system availability sensitivity; or (ii) 3 business days of failure for systems with a High system availability sensitivity*] of failure.

Supplemental Guidance: Organizations specify the information subsystem components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	Assessed Status:	

MP-1 Media Protection Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*Chief Information Officer (CIO); Chief Information Security Officer (CISO);Designated Approving Authority (DAA); Director, Office of Information Services (OIS); system information subsystem security officers (ISSOs); system owners*]: (i) a media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. reviews and updates [*as needed*] the current: (i) media protection policy [*at least annually*]; and (ii) media protection procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	Assessed Status:	

MP-2 Media Access

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization restricts access to [*backup media; flash/thumb drives; mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices)*] to [*system administrators (backup media only); system administrators and device users (flash/thumb drives; mobile computing and communications devices with information storage capability)*].

Supplemental Guidance: Information subsystem media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper, and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-111.

Main Control Implementation Detail	**Assessed Status:**	

MP-3 Media Marking

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. marks information subsystem media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. exempts [*Sensitive Unclassified Non-Safeguards Information (SUNSI) internal hard drives; SUNSI external hard drives, CDs / DVDs; SUNSI flash/thumb drives*] from marking as long as the media remain within [*areas approved for the open storage of the information residing on the media as long as the information is considered available to all NRC users.*].

Supplemental Guidance: The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information subsystems (see AC-16). Information subsystem media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper, and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information subsystem media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: AC-16, PL-2, RA-3.

Control Enhancements: None.

References: FIPS Publication 199.

Main Control Implementation Detail	**Assessed Status:**	

MP-4 Media Storage

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. physically controls and securely stores [*digital media and non-digital media*] within [(digital media) *specified controlled areas in accordance with CSO-STD-2004, "Electronic Media and Device Handling" and (non-digital media) specified controlled areas in accordance with NRC Management Directive (MD) 12.1, "NRC Facility Security Program," MD 12.2, "NRC Classified Information Security Program," MD 12.7, "NRC Safeguards Information Security Program," MD 12.6, "NRC Sensitive Unclassified Information Security Program," and "NRC Policy and Procedures for Handling, Marking, and Protecting SUNSI," available on the internal NRC Security Web site http://www.internal.nrc.gov/security.html*]; and

b. protects information subsystem media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: Information subsystem media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper, and microfilm. Physically controlling information subsystem media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information subsystems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.

Main Control Implementation Detail	**Assessed Status:**	

MP-5 Media Transport

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. protects and controls [*digital media and non-digital media*] during transport outside of controlled areas using [(digital media) *specified controlled areas in accordance with CSO-STD-2004, "Electronic Media and Device Handling." (non-digital media) and specified controlled areas in accordance with NRC Management Directive (MD) 12.1, "NRC Facility Security Program," MD 12.2, "NRC Classified Information Security Program," MD 12.7, "NRC Safeguards Information Security Program," MD 12.6, "NRC Sensitive Unclassified Information Security Program," and "NRC Policy and Procedures for Handling, Marking, and Protecting SUNSI," available on the internal NRC Security Web site http://www.internal.nrc.gov/security.html*];

b. maintains accountability for information subsystem media during transport outside of controlled areas;

c. documents activities associated with the transport of information subsystem media; and

d. restricts the activities associated with the transport of information subsystem media to authorized personnel.

Supplemental Guidance: Information subsystem media includes both digital and non-digital media. Digital media

includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper, and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information subsystems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information subsystem media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

References: FIPS Publication 199; NIST Special Publication 800-60.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 4: Media Transport | Cryptographic Protection

The information subsystem implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Supplemental Guidance: This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Related control: MP-2.

Control Enhancement 4 Implementation Detail	**Assessed Status:**	

MP-6 Media Sanitization

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. sanitizes [*SUNSI, Safeguards Information (SGI), and Classified information*] prior to disposal, release out of organizational control, or release for reuse using [*media sanitization techniques and procedures defined in CSO-STD-2004, "Electronic Media and Device Handling"*] in accordance with applicable federal and organizational standards and policies; and

b. employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance: This control applies to all information subsystem media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods

cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Media Sanitization | Review / Approve / Track / Document / Verify

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Supplemental Guidance: Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. Related control: SI-12.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 2: Media Sanitization | Equipment Testing

The organization tests sanitization equipment and procedures [*at least annually*] to verify that the intended sanitization is being achieved.

Supplemental Guidance: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 3: Media Sanitization | Nondestructive Techniques

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information subsystem under the following circumstances: [*(i) upon initial purchase; (ii) when the device has been outside the control of the user or authorized individual; (iii) if there is a belief that the device may contain malicious code; if the device has been connected to an untrusted system; or (iv) when the device returns from travel outside the U.S.*].

Supplemental Guidance: This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information subsystems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information subsystems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

MP-7 Media Use

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization [*prohibits*] the use of [*personally owned, removable media*] on [*information subsystems*] in accordance with [*"NRC Agency-wide Rules of Behavior for Authorized Computer Use" and CSO-STD-1004, "Laptop Security Standard."*].

Supplemental Guidance: Information subsystem media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper, and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information subsystems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information subsystem media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Related controls: AC-19, PL-4.

References: FIPS Publication 199; NIST Special Publication 800-111.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Media Use | Prohibit Use Without Owner

The organization prohibits the use of portable storage devices in organizational information subsystems when such devices have no identifiable owner.

Supplemental Guidance: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion). Related control: PL-4.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

PE-1 Physical and Environmental Protection Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*CIO, CISO, DAA, IT executive, IT manager, IT functional manager, IT systems development official, IT auditor, system owners, ISSOs, office ISSOs, system administrators (e.g., database, network), facility owners, physical security officers*]: (i) a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

b. reviews and updates [*as needed*] the current: (i) physical and environmental protection policy [*at least annually*]; and (ii) physical and environmental protection procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

PE-2 Physical Access Authorizations

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, approves, and maintains a list of individuals with authorized access to the facility where the information subsystem resides;

b. issues authorization credentials for facility access;

c. reviews the access list detailing authorized facility access by individuals [*at least annually*]; and

d. removes individuals from the facility access list when access is no longer required.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. Related controls: PE-3, PE-4, PS-3.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PE-3 Physical Access Control

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. enforces physical access authorizations at [*all entry/exit points to the facility where the information subsystem resides to include interior access points for components requiring supplemental access controls*] by: (i) verifying individual access authorizations before granting access to the facility; and (ii) controlling ingress/egress to the facility using [*physical access control systems/devices such as card readers, locks, keys, alarms, cameras, and/or guards.*];

b. maintains physical access audit logs for [*all entry/exit points to the facility where the information subsystem resides to include interior access points for components requiring supplemental access controls*];

c. provides [*guards, gates, cameras, and alarms*] to control access to areas within the facility officially designated as publicly accessible;

d. escorts visitors and monitors visitor activity [*at all times while within an NRC-controlled space*];

e. secures keys, combinations, and other physical access devices;

f. inventories [*physical access card readers, locks, keys, alarms, and cameras at least annually*]; and

g. changes combinations and keys [*in accordance with MD 12.1*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff, or other personnel such as administrative staff or information subsystem users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information subsystems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information subsystems and/or components requiring supplemental access controls, or both. Components of organizational information subsystems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoD Instruction 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: http://idmanagement.gov, http://fips201ep.cio.gov.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Physical Access Control | Information subsystem Access

The organization enforces physical access authorizations to the information subsystem [*(excluding end user devices)*] in addition to the physical access controls for the facility [*where there is a concentration of information subsystem components (i.e., server rooms, media storage areas, wiring closets, and data centers).*].

Supplemental Guidance: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information subsystem components (e.g., server rooms, media storage areas, data, and communications centers). Related control: PS-2.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

PE-4 Access Control for Transmission Medium

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization controls physical access to [*information subsystem distribution and transmission lines (i.e., cabling, phone, power)*] within organizational facilities using [(i) *locked wiring closets or telephone closets; (ii) disconnected or locked spare jacks; (iii) protection of cabling by conduit or cable trays; and (iv) alarms*].

Supplemental Guidance: Physical security safeguards applied to information subsystem distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical

safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8. Control Enhancements: None. References: NSTISSI No. 7003.		
Main Control Implementation Detail	**Assessed Status:**	

PE-5 Access Control for Output Devices

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**
Main Control: The organization controls physical access to information subsystem output devices to prevent unauthorized individuals from obtaining the output. Supplemental Guidance: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information subsystem output devices. Related controls: PE-2, PE-3, PE-4, PE-18. Control Enhancements: None. References: None.		
Main Control Implementation Detail	**Assessed Status:**	

PE-6 Monitoring Physical Access

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**
Main Control: The organization: a. monitors physical access to the facility where the information subsystem resides to detect and respond to physical security incidents; b. reviews physical access logs [*daily*] and upon occurrence of [*a security incident or suspicious physical access activities, including: (i) accesses outside of normal work hours; (ii) two or more access attempts to areas not normally accessed; and (iii) demonstrations or disturbances outside the building.*]; and c. coordinates results of reviews and investigations with the [*system owner and CSIRT*]. Supplemental Guidance: Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8. References: None.		
Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**	
Control Enhancement 1: Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment The organization monitors physical intrusion alarms and surveillance equipment. Supplemental Guidance: None.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**	
Control Enhancement 4: Monitoring Physical Access | Monitoring Physical Access to Information subsystems The organization monitors physical access to the information subsystem in addition to the physical access monitoring of the facility [*where there is a concentration of information subsystem components (i.e., server rooms, media storage areas, wiring closets, and data centers)*]. Supplemental Guidance: This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information subsystem components (e.g., server rooms, media storage areas, communications centers). Related controls: PS-2, PS-3.		
Control Enhancement 4 Implementation Detail	**Assessed Status:**	

PE-8 Visitor Access Records

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:	**Hybrid**	
Main Control: The organization: a. maintains visitor access records to the facility where the information subsystem resides [*in accordance with the NARA GRS*]; and b. reviews visitor access records [*at least daily for all systems*]. Supplemental Guidance: Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas. References: None.		
Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**	
Control Enhancement 1: Visitor Access Records | Automated Records Maintenance / Review The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records. Supplemental Guidance: None.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

PE-9 Power Equipment and Cabling

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization protects power equipment and power cabling for the information subsystem from damage and destruction.

Supplemental Guidance: Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling, and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites. Related control: PE-4.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PE-10 Emergency Shutoff

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. provides the capability of shutting off power to the information subsystem or individual system components in emergency situations;

b. places emergency shutoff switches or devices in [*server rooms, rooms with online storage media (e.g., Storage Area Networks [SAN]), and data centers*] to facilitate safe and easy access for personnel; and

c. protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information subsystem resources including, for example, data centers, server rooms, and mainframe computer rooms. Related control: PE-15.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PE-11 Emergency Power

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization provides a short-term uninterruptible power supply to facilitate [*(i) an orderly shutdown of systems for Low and Moderate sensitivity systems; (ii) transition of the information subsystem to long-term alternate power for High sensitivity systems*] in the event of a primary power source loss.

Supplemental Guidance: Related controls: AT-3, CP-2, CP-7.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**
Control Enhancement 1: Emergency Power | Long-Term Alternate Power Supply - Minimal Operational Capability The organization provides a long-term alternate power supply for the information subsystem that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source. Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information subsystem can be either manually or automatically activated.	

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

PE-12 Emergency Lighting

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**
Main Control: The organization employs and maintains automatic emergency lighting for the information subsystem that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. Supplemental Guidance: This control applies primarily to facilities containing concentrations of information subsystem resources including, for example, data centers, server rooms, and mainframe computer rooms. Related controls: CP-2, CP-7. Control Enhancements: None. References: None.		

Main Control Implementation Detail	**Assessed Status:**	

PE-13 Fire Protection

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**
Main Control: The organization employs and maintains fire suppression and detection devices/systems for the information subsystem that are supported by an independent energy source. Supplemental Guidance: This control applies primarily to facilities containing concentrations of information subsystem resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. References: None.		

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**
Control Enhancement 1: Fire Protection | Detection Devices / Systems	

The organization employs fire detection devices/systems for the information subsystem that activate automatically and notify the [*facility central alarm station*] and [*the local fire and rescue service*] in the event of a fire. Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information subsystems containing classified information.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 2: Fire Protection | Suppression Devices / Systems The organization employs fire suppression devices/systems for the information subsystem that provide automatic notification of any activation to the [*facility central alarm station*] and [*the local fire and rescue service*]. Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information subsystems containing classified information.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 3: Fire Protection | Automatic Fire Suppression The organization employs an automatic fire suppression capability for the information subsystem when the facility is not staffed on a continuous basis. Supplemental Guidance: None.		
Control Enhancement 3 Implementation Detail	**Assessed Status:**	

PE-14 Temperature and Humidity Controls

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**Hybrid**	
Main Control: The organization: a. maintains temperature levels within the facility where the information subsystem resides at [*68 °Fahrenheit (F) and 75 °F, with an early warning provided at 80 °F and a critical alert provided at 85 °F*]; b. maintains humidity levels within the facility where the information subsystem resides at [*ambient relative humidity levels between 45% and 55%, with early warnings provided at 40% and 60% relative humidity and critical alerts provided at 30% and 70% relative humidity*]; c. monitors temperature and humidity levels [*in real time*]. Supplemental Guidance: This control applies primarily to facilities containing concentrations of information subsystem resources, for example, data centers, server rooms, and mainframe computer rooms. Related control: AT-3. Control Enhancements: None. References: None.		
Main Control Implementation Detail	**Assessed Status:**	

PE-15 Water Damage Protection

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization protects the information subsystem from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information subsystem resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations. Related control: AT-3.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Water Damage Protection | Automation Support

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information subsystem and alerts [*facility personnel*].

Supplemental Guidance: Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

PE-16 Delivery and Removal

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

The organization authorizes, monitors, and controls [*all computer hardware*] entering and exiting the facility and maintains records of those items [*in accordance with MD 12.5 and MD and Handbook 13.1, "Property Management"*].

.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information subsystem components may require restricting access to delivery areas and possibly isolating the areas from the information subsystem and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PE-17 Alternate Work Site

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. employs [*computer security controls consistent with MD 12.5 and CSO standards, processes, procedures, templates, and checklists*] at alternate work sites;

b. assesses as feasible, the effectiveness of security controls at alternate work sites; and

c. provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative. Related controls: AC-17, CP-7.

Control Enhancements: None.

References: NIST Special Publication 800-46.

Main Control Implementation Detail	**Assessed Status:**	

PE-18 Location of Information subsystem Components

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**System-Specific**

Main Control: The organization positions information subsystem components within the facility to minimize potential damage from [*sprinklers, water pipes, extreme weather, and hazardous spills*] and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information subsystems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PL-1 Security Planning Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*Chief Information Officer (CIO); Chief Information Security Officer (CISO); Designated Approving Authority (DAA); Director, Office of Information Services (OIS); system information subsystem security officers (ISSO); system owners*]: (i) a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

b. reviews and updates [*as needed*] the current: (i) security planning policy [*at least annually*]; and (ii) security planning procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

PL-2 System Security Plan

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. develops a security plan for the information subsystem that: (i) is consistent with the organization's enterprise architecture; (ii) explicitly defines the authorization boundary for the system; (iii) describes the operational context of the information subsystem in terms of missions and business processes; (iv) provides the security categorization of the information subsystem including supporting rationale; (v) describes the operational environment for the information subsystem and relationships with or connections to other information subsystems; (vi) provides an overview of the security requirements for the system; (vii) identifies any relevant overlays, if applicable; (viii) describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and (ix) is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. distributes copies of the security plan and communicates subsequent changes to the plan to [*CISO; CSO senior information technology security officer (SITSO) with responsibility for continuous monitoring oversight; system administrators; system ISSO*];

c. reviews the security plan for the information subsystem [*at least quarterly*];

d. updates the plan to address changes to the information subsystem/environment of operation or problems identified during plan implementation or security control assessments; and

e. protects the security plan from unauthorized disclosure and modification.

Supplemental Guidance: Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction1253 to develop overlays for community-wide use or to address specialized

requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays.

Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

References: NIST Special Publication 800-18.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 3: System Security Plan | Plan / Coordinate with Other Organizational Entities

The organization plans and coordinates security-related activities affecting the information subsystem with [*CISO; CSO SITSO with responsibility for continuous monitoring oversight; office directors; system ISSO; system administrators (e.g., database, network); system users*] before conducting such activities in order to reduce the impact on other organizational entities.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information subsystems or other documents, as appropriate. Related controls: CP-4, IR-4.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

PL-4 Rules of Behavior

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.

Control Type:	**Hybrid**

Main Control: The organization:

a. establishes and makes readily available to individuals requiring access to the information subsystem, the rules that describe their responsibilities and expected behavior with regard to information and information subsystem usage;

b. receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information subsystem;

c. reviews and updates the rules of behavior [*at least annually*]; and

d. requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Supplemental Guidance: This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information subsystems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8,

System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.

References: NIST Special Publication 800-18.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Rules of Behavior | Social Media and Networking Restrictions

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Supplemental Guidance: This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information subsystems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

PL-8 Information Security Architecture

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. develops an information security architecture for the information subsystem that: (i) describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; (ii) describes how the information security architecture is integrated into and supports the enterprise architecture; and (iii) describes any information security assumptions about, and dependencies on, external services; and

b. reviews and updates the information security architecture [*at least annually*] to reflect updates in the enterprise architecture; and

c. ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Supplemental Guidance: This control addresses actions taken by organizations in the design and development of information subsystems. The information security architecture at the individual information subsystem level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information subsystem, restoration priorities of information and information subsystem services, and any other specific protection needs.

In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information subsystems is critical to implementing and maintaining an effective

information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information subsystem, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information subsystems or information subsystem components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PM-1 Information Security Program Plan

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. develops and disseminates an organization-wide information security program plan that: (i) provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; (ii) includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; (iii) reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and (iv) is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. reviews the organization-wide information security program plan [*at least annually*];

c. updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and

d. protects the information security program plan from unauthorized disclosure and modification.

Supplemental Guidance: Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.

The security plans for individual information subsystems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information subsystem (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information subsystems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information subsystem but instead, support multiple information subsystems.

Related control: PM-8. Control Enhancements: None. References: None.		
Main Control Implementation Detail	**Assessed Status:**	

PM-2 Senior Information Security Officer

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control:

The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PM-3 Information Security Resources

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and

c. ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Control Enhancements: None.

References: NIST Special Publication 800-65.

Main Control Implementation Detail	**Assessed Status:**	

PM-4 Plan of Action and Milestones Process

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information subsystems: (i) are developed and maintained; (ii) document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and (iii) are reported in accordance with OMB FISMA reporting requirements.

b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information subsystem), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5.

Control Enhancements: None.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

Main Control Implementation Detail	**Assessed Status:**	

PM-5 Information subsystem Inventory

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control:

The organization develops and maintains an inventory of its information subsystems.

Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information subsystems inventories and associated reporting requirements. For specific information subsystem inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.

Control Enhancements: None.

References: Web: http://www.omb.gov.

Main Control Implementation Detail	**Assessed Status:**	

PM-6 Information Security Measures of Performance

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control:

The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

Control Enhancements: None. References: NIST Special Publication 800-55.		
Main Control Implementation Detail	**Assessed Status:**	

PM-7 Enterprise Architecture

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control:

The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral information security architecture consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information subsystems. For PL-8, the information security architecture is developed at a level representing an individual information subsystem but at the same time, is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PL-8, PM-11, RA-2, SA-3.

Control Enhancements: None.

References: NIST Special Publication 800-39.

Main Control Implementation Detail	**Assessed Status:**	

PM-8 Critical Infrastructure Plan

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control:

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance: Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.

Control Enhancements: None.

References: HSPD 7; National Infrastructure Protection Plan.

Main Control Implementation Detail	**Assessed Status:**	

PM-9 Risk Management Strategy

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information subsystems;

b. implements the risk management strategy consistently across the organization; and

c. reviews and updates the risk management strategy [*at least annually*] or as required, to address organizational changes.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.

Control Enhancements: None.

References: NIST Special Publications 800-30, 800-39.

Main Control Implementation Detail	**Assessed Status:**	

PM-10 Security Authorization Process

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. manages (i.e., documents, tracks, and reports) the security state of organizational information subsystems and the environments in which those systems operate through security authorization processes;

b. designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. fully integrates the security authorization processes into an organization-wide risk management program.

Supplemental Guidance: Security authorization processes for information subsystems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information subsystem and common control provider. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation. Related control: CA-6.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-39.

Main Control Implementation Detail	**Assessed Status:**	

PM-11 Mission/Business Process Definition

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information subsystems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-60.

Main Control Implementation Detail	**Assessed Status:**	

PM-12 Insider Threat Program

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control:

The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

Supplemental Guidance: Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information subsystem security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines. Related

controls: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14. Control Enhancements: None. References: Executive Order 13587.		
Main Control Implementation Detail	**Assessed Status:**	

PM-13 Information Security Workforce

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control:

The organization establishes an information security workforce development and improvement program.

Supplemental Guidance: Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals. Related controls: AT-2, AT-3.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PM-14 Testing, Training, and Monitoring

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information subsystems: (i) are developed and maintained; and (ii) continue to be executed in a timely manner;

b. reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance: This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information subsystems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments. Related controls: AT-3, CA-7, CP-4, IR-3, SI-4.

Control Enhancements: None.

References: NIST Special Publications 800-16, 800-37, 800-53A, 800-137.		
Main Control Implementation Detail	**Assessed Status:**	

PM-15 Contacts with Security Groups and Associations

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:

a. to facilitate ongoing security education and training for organizational personnel;

b. to maintain currency with recommended security practices, techniques, and technologies; and

c. to share current security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related control: SI-5.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PM-16 Threat Awareness Program

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control:

The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

Supplemental Guidance: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information subsystems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared. Related controls: PM-12, PM-16.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

PS-1 Personnel Security Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**<Common>**

Main Control: The organization:

e. develops, documents, and disseminates to [*Chief Information Officer (CIO); Chief Information Security Officer (CISO); Designated Approving Authority (DAA); Director, Office of Administration (ADM); Computer Security Office (CSO) Senior Information Technology Security Officer (SITSO) with responsibility for continuous monitoring oversight; Director, Office of Information Services (OIS); system information subsystem security officers (ISSOs); office ISSOs; system owners*]: (i) a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

f. reviews and updates [*as needed*] the current: (i) personnel security policy [*at least annually*]; and (ii) personnel security procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

PS-2 Position Risk Designation

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**<Common>**

Main Control: The organization:

a. assigns a risk designation to all organizational positions;

b. establishes screening criteria for individuals filling those positions; and

c. reviews and updates position risk designations [*in accordance with Management Directive (MD) 12.3, "NRC Personnel Security Program"*].

Supplemental Guidance: Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information subsystems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances). Related controls: AT-3, PL-2, PS-3.

Control Enhancements: None.

References: 5 C.F.R. 731.106.

Main Control Implementation Detail	**Assessed Status:**	

PS-3 Personnel Screening

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. screens individuals prior to authorizing access to the information subsystem; and

b. re-screens individuals according to [*in accordance with MD 12.3, "NRC Personnel Security Program."*].

Supplemental Guidance: Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information subsystems based on types of information processed, stored, or transmitted by the systems. Related controls: AC-2, IA-4, PE-2, PS-2.

Control Enhancements: None.

References: 5 C.F.R. 731.106; FIPS Publications 199, 201; NIST Special Publications 800-60, 800-73, 800-76, 800-78; ICD 704.

Main Control Implementation Detail	**Assessed Status:**	

PS-4 Personnel Termination

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization, upon termination of individual employment:

a. disables information subsystem access [*on the last day of employment for voluntary terminations and prior to user notification for involuntary terminations*];

b. terminates/revokes any authenticators/credentials associated with the individual;

c. conducts exit interviews that include a discussion of [*security topics defined in NRC Form 136, "Security Termination Statement," and system specific security considerations*];

d. retrieves all security-related organizational information subsystem-related property;

e. retains access to organizational information and information subsystems formerly controlled by terminated individual; and

f. notifies [*ADM/Division of Facilities and Security (DFS)/Personnel Security Branch (PSB)*] within [*5 calendar days prior to the last day of employment*].

Supplemental Guidance: Information subsystem-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information subsystem-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information subsystem accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**<Common>**

Control Enhancement 2: Personnel Termination | Automated Notification

The organization employs automated mechanisms to notify [*system owners and facility owners*] upon termination of an individual.

Supplemental Guidance: In organizations with a large number of employees, not all personnel who need to know about termination actions receive the appropriate notifications—or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles (e.g., management personnel, supervisors, personnel security officers, information security officers, systems administrators, or information technology administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

PS-5 Personnel Transfer

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. reviews and confirms ongoing operational need for current logical and physical access authorizations to information subsystems/facilities when individuals are reassigned or transferred to other positions within the organization;

b. initiates the following actions [*within 5 business days:*

Physical Access:

- *Review existing facility access authorizations and remove access no longer required in the new position.*
- *Collect keys/building passes when the personnel no longer require access to those locations to perform new position functions.*
- *Modify facility access codes when personnel no longer require access to those locations to perform new position functions.*
- *Collect identification cards when personnel no longer require them to perform new position functions;*

Logical Access:

- *Review existing systems access authorizations and removing access no longer required in the new position;*
- *Collect mobile devices when personnel no longer require the devices to perform new position functions; and*
- *Disable old accounts no longer required to perform new position functions.*]

c. modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. notifies [*system owners and facility owners*] within [*at least 5 calendar days prior to the transfer*].

Supplemental Guidance: This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information subsystem accounts and establishing new accounts; (iii) changing information subsystem access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information subsystem accounts. Related controls: AC-2, IA-4, PE-2, PS-4.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	Assessed Status:	

PS-6 Access Agreements

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops and documents access agreements for organizational information subsystems;

b. reviews and updates the access agreements [*at least annually*]; and

c. ensures that individuals requiring access to organizational information and information subsystems: (i) sign appropriate access agreements prior to being granted access; and (ii) re-sign access agreements to maintain access to organizational information subsystems when access agreements have been updated or [*at least every 2 years*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information subsystems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	Assessed Status:	

PS-7 Third-Party Personnel Security

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. requires third-party providers to comply with personnel security policies and procedures established by the organization;

c. documents personnel security requirements;

d. requires third-party providers to notify the [*Contracting Officers Representative (COR)*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information subsystem privileges, within [*2 business days of the transfer date or the last day of employment*]; and

e. monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information subsystem development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information subsystem privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

Control Enhancements: None. References: NIST Special Publication 800-35.		
Main Control Implementation Detail	**Assessed Status:**	

PS-8 Third-Party Personnel Security

Implementation Priority:	P3	This control relies on functionality provided by P1 and P2 controls. It should be implemented after P1 and P2 controls.
Control Type:		**<Common>**

Main Control: The organization:

a. employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

b. notifies [*system owners and facility owners*] within [*1 business day*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Supplemental Guidance: Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

RA-1 Risk Assessment Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*Chief Information Officer (CIO); Chief Information Security Officer (CISO); Designated Approving Authority (DAA); Computer Security Office (CSO) senior information technology security officer (SITSO) with responsibility for continuous monitoring oversight; Director, Office of Information Services (OIS); system information subsystem security officers (ISSOs); system owners*]: (i) a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. reviews and updates the current: (i) risk assessment policy [*at least annually*]; and (ii) risk assessment procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-100.		
Main Control Implementation Detail	**Assessed Status:**	

RA-2 Security Categorization

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. categorizes information and the information subsystem in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. documents the security categorization results (including supporting rationale) in the security plan for the information subsystem; and

c. ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information subsystems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information subsystem owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information subsystem components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Main Control Implementation Detail	**Assessed Status:**	

RA-3 Risk Assessment

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information subsystem and the information it processes, stores, or transmits;

b. documents risk assessment results in [*accordance with CSO cyber-security requirements*];

c. reviews and updates risk assessment results [*at least every year*];

d. disseminates risk assessment results to [*CISO; DAA; CSO SITSO with responsibility for continuous monitoring oversight; system ISSO*]; and

e. conducts a new risk assessment [*at least every 3 years*] or whenever there are significant changes to the information subsystem or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective risk assessments.

Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information subsystems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information subsystems on behalf of the organization, individuals accessing organizational information subsystems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information subsystems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information subsystems.

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information subsystem level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information subsystem authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9.

Control Enhancements: None.

References: OMB Memorandum 04-04; NIST Special Publication 800-30, 800-39; Web: http://idmanagement.gov.

Main Control Implementation Detail	**Assessed Status:**	

RA-5 Vulnerability Scanning

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. scans for vulnerabilities in the information subsystem and hosted applications [*at least quarterly for non-NSS*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: (i) enumerating platforms, software flaws, and improper configurations; (ii) formatting checklists and test procedures; and (iii) measuring vulnerability impact;

c. analyzes vulnerability scan reports and results from security control assessments;

d. remediates legitimate vulnerabilities in accordance with an organizational assessment of risk and the following timeframes: [*(i) critical findings within 21 calendar days; (ii) high risk findings within 45 calendar days; (iii) moderate risk findings within 90 calendar days; and (iv) low risk findings within 120 calendar days*]; and

e. shares information obtained from the vulnerability scanning process and security control assessments with [*CISO; DAA; CSO SITSO with responsibility for continuous monitoring oversight; Director, OIS; and system ISSO*] to help eliminate similar vulnerabilities in other information subsystems (i.e., systemic weaknesses or deficiencies).

Supplemental Guidance: Security categorization of information subsystems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information subsystem components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the

Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

References: NIST Special Publications 800-40, 800-70, 800-115; Web: http://cwe.mitre.org, http://nvd.nist.gov.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Vulnerability Scanning | Update Tool Capability

The organization employs vulnerability scanning tools that include the capability to readily update the information subsystem vulnerabilities to be scanned.

Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information subsystem are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 2: Vulnerability Scanning | Update By Frequency / Prior To New Scan / When Identified

The organization updates the information subsystem vulnerabilities scanned [*at least quarterly for non-NSS*].

Supplemental Guidance: Related controls: SI-3, SI-5.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 4: Vulnerability Scanning | Discoverable Information

The organization determines what information about the information subsystem is discoverable by adversaries and subsequently takes the following actions: [*modifies the system to make designated information less relevant or attractive to adversaries; or removes designated information*].

Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information subsystem, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information subsystem to make designated information less relevant or attractive to adversaries. Related control: AU-13.

Control Enhancement 4 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 5: Vulnerability Scanning | Privileged Access

The information subsystem implements privileged access authorization to [*all host-based vulnerability scans*] for selected [*thorough vulnerability scanning*].

Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the information subsystem component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.

Control Enhancement 5 Implementation Detail	**Assessed Status:**	

SA-1 System and Services Acquisition Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*CIO, CISO, DAA, IT executive, IT manager, IT functional manager, IT systems development official, IT auditor, system owners, ISSOs, office ISSOs, system administrators (e.g., database, network)*]: (i) a system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. reviews and updates [*as needed*] the current: (i) system and services acquisition policy [*at least annually*]; and (ii) system and services acquisition procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

SA-2 Allocation of Resources

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. determines information security requirements for the information subsystem or information subsystem service in mission/business process planning;

b. determines, documents, and allocates the resources required to protect the information subsystem or information subsystem service as part of its capital planning and investment control process; and

c. establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Resource allocation for information security includes funding for the initial information subsystem or information subsystem service acquisition and funding for the sustainment of the system/service. Related controls: PM-3, PM-11.

Control Enhancements: None.

References: NIST Special Publication 800-65.

Main Control Implementation Detail	**Assessed Status:**	

SA-3 System Development Life Cycle

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. manages the information subsystem using [*the MD 2.8, "Project Management Methodology (PMM)," for system development life cycle activities*] that incorporates information security considerations;

b. defines and documents information security roles and responsibilities throughout the system development life cycle;

c. identifies individuals having information security roles and responsibilities; and

d. integrates the organizational information security risk management process into system development life cycle activities.

Supplemental Guidance: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information subsystems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information subsystems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information subsystem security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information subsystems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information subsystem. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-64.

Main Control Implementation Detail	**Assessed Status:**	

SA-4 Acquisition Process

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information subsystem, system component, or information subsystem service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. security functional requirements;

b. security strength requirements;

c. security assurance requirements;

d. security-related documentation requirements;

e. requirements for protecting security-related documentation;

f. description of the information subsystem development environment and environment in which the system is intended to operate; and

g. acceptance criteria.

Supplemental Guidance: Information subsystem components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information subsystem. Information subsystem components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information subsystem and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information subsystems, information subsystem components, and information subsystem services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: http://www.niap-ccevs.org, http://fips201ep.cio.gov, http://www.acquisition.gov/far.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Acquisition Process | Functional Properties of Security Controls

The organization requires the developer of the information subsystem, system component, or information subsystem service to provide a description of the functional properties of the security controls to be employed.

Supplemental Guidance: Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Acquisition Process | Design / Implementation Information for Security Controls

The organization requires the developer of the information subsystem, system component, or information subsystem service to provide design and implementation information for the security controls to be employed that includes: [*the following at a sufficient level of detail: (i) security-relevant external system interfaces; (ii) high-level design; (iii) low-level design; and (iv) source code with sufficient detail to allow for analysis and testing of security controls to meet overall risk response expectations*].

Supplemental Guidance: Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information subsystems, system components, or information subsystem services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information subsystems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant

functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information subsystem. Related control: SA-5.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 9: Acquisition Process | Functions / Ports / Protocols / Services In Use The organization requires the developer of the information subsystem, system component, or information subsystem service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. Supplemental Guidance: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information subsystem, information subsystem component, or information subsystem service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information subsystem service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information subsystem, system component, or information subsystem service has been implemented. SA-9 describes requirements for external information subsystem services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.		
Control Enhancement 9 Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 10: Acquisition Process | Use Of Approved PIV Products The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information subsystems. Supplemental Guidance: Related controls: IA-2; IA-8.		
Control Enhancement 10 Implementation Detail	**Assessed Status:**	

SA-5 Information subsystem Documentation

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:	**System-Specific**	

Main Control: The organization:

a. Obtains administrator documentation for the information subsystem, system component, or information subsystem service that describes: (i) secure configuration, installation, and operation of the system, component, or service; (ii) effective use and maintenance of security functions/mechanisms; and (iii) known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information subsystem, system component, or information subsystem service that describes: (i) user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; (ii) methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and (iii) user responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information subsystem, system component, or information subsystem service documentation when such documentation is either unavailable or nonexistent and [*notifies the DAA so*

appropriate actions can be taken] in response;

d. Protects documentation as required, in accordance with [*CSO-PROS-2030 "NRC Risk Management Framework (RMF) and Authorization Process"*]; and

e. Distributes documentation to [*appropriate stakeholders and system administrators that have a valid need-to-know*].

Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information subsystems, system components, and information subsystem services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information subsystem/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information subsystem, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information subsystem vulnerabilities may also require an increased level of protection. Secure operation of the information subsystem, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	Assessed Status:	

SA-8 Security Engineering Principles

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization applies information subsystem security engineering principles in the specification, design, development, implementation, and modification of the information subsystem.

Supplemental Guidance: Organizations apply security engineering principles primarily to new development information subsystems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

Control Enhancements: None.

References: NIST Special Publication 800-27.

Main Control Implementation Detail	Assessed Status:	

SA-9 External Information subsystem Services

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. requires that providers of external information subsystem services comply with [*all federally mandated and NRC-defined cyber security requirements*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. defines and documents government oversight and user roles and responsibilities with regard to external information subsystem services; and

c. employs [*the following processes: (i) carry out day-to-day security operations of the interconnected system(s) to include periodic vulnerability assessment scanning, annual contingency plan testing, and annual control testing, etc; and (ii) ensure the requirements detailed in the Cybersecurity Risk Management Activities Instructions are met for all external systems*] to monitor security control compliance by external service providers on an ongoing basis.

Supplemental Guidance: External information subsystem services are services that are implemented outside of the authorization boundaries of organizational information subsystems. This includes services that are used by, but not a part of, organizational information subsystems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information subsystems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information subsystem services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information subsystem services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.

References: NIST Special Publication 800-35.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: External Information subsystems | Identification of Functions / Ports / Protocols / Services

The organization requires providers of [*NRC-approved external information subsystem services*] to identify the functions, ports, protocols, and other services required for the use of such services.

Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols. Related control: CM-7.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

SA-10 Developer Configuration Management

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization requires the developer of the information subsystem, system component, or information subsystem service to:

a. perform configuration management [*as defined in MD 12.5 and MD 2.8*] during system, component, or service [*inception, construction, transition, operation and maintenance, and retirement*];

b. document, manage, and control the integrity of changes to [*hardware, software, firmware, and documentation*];

c. implement only organization-approved changes to the system, component, or service;

d. document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. track security flaws and flaw resolution within the system, component, or service and report findings to [*system owner, system ISSO, and system administrators*].

Supplemental Guidance: This control also applies to organizations conducting internal information subsystems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information subsystem, information subsystem component, or information subsystem service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.

Control Enhancements: None.

References: NIST Special Publication 800-128.

Main Control Implementation Detail	**Assessed Status:**	

SA-11 Developer Security Testing and Evaluation

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization requires the developer of the information subsystem, system component, or information subsystem service to:

a. create and implement a security assessment plan;

b. perform [*unit, integration, system, and regression*] testing/evaluation at [*all post-design phases of the system development life cycle*];

c. produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. implement a verifiable flaw remediation process; and

e. correct flaws identified during security testing/evaluation.

Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements.

Security properties of information subsystems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information subsystem. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Control Enhancements: None.

References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: http://nvd.nist.gov, http://cwe.mitre.org, http://cve.mitre.org, http://capec.mitre.org.

Main Control Implementation Detail	**Assessed Status:**	

SA-12 Supply Chain Protection

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization protects against supply chain threats to the information subsystem, system component, or information subsystem service by employing [*security impact analysis on vendors, suppliers, and countries of origin in the supply chain to ensure that system components are not manufactured with embedded spyware or by incorporating counterfeit elements*] as part of a comprehensive, defense-in-breadth information security strategy [*in accordance with NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information subsystems and Organizations"*].

Supplemental Guidance: Information subsystems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information subsystems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information subsystems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information subsystems and information subsystem components, prior to taking delivery of such systems/components. This control enhancement also applies to information subsystem services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information subsystem. Contracts may specify documentation protection requirements. Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.

Control Enhancements: None.

References: NIST Special Publication 800-161; NIST Interagency Report 7622.

Main Control Implementation Detail	Assessed Status:	

SA-15 Development Process, Standards, and Tools

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. Requires the developer of the information subsystem, system component, or information subsystem service to follow a documented development process that: (i) explicitly addresses security requirements; (ii) identifies the standards and tools used in the development process; (iii) documents the specific tool options and tool configurations used in the development process; and (iv) documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Reviews the development process, standards, tools, and tool options/configurations [*at least quarterly*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*established agency-wide CM processes and procedures*].

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	Assessed Status:	

SA-16 Developer-Provided Training

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization requires the developer of the information subsystem, system component, or information subsystem service to provide [*annual security role-based training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Supplemental Guidance: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information subsystems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms. Related controls: AT-2, AT-3, SA-5.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	Assessed Status:	

SA-17 Developer Security Architecture and Design

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization requires the developer of the information subsystem, system component, or information subsystem service to produce a design specification and security architecture that:

a. is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;

b. accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

c. expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Supplemental Guidance: This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information subsystems, information subsystem components, or information subsystem services to external entities, and there is a requirement to demonstrate consistency with the organization's enterprise architecture and information security architecture. Related controls: PL-8, PM-7, SA-3, SA-8.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SC-1 System and Communications Protection Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*CIO, CISO, Designated Accrediting Authority (DAA), IT executive, IT manager, IT functional manager, IT systems development official, IT auditor, system owners, ISSOs, office ISSOs, system administrators (e.g., database, network)*]: (i) a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. reviews and updates [*as needed*] the current: (i) System and communications protection policy [*at least annually*]; and (ii) system and communications protection procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	Assessed Status:	

SC-2 Application Partitioning

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem separates user functionality (including user interface services) from information subsystem management functionality.

Supplemental Guidance: Information subsystem management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information subsystem management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information subsystem resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	Assessed Status:	

SC-3 Security Function Isolation

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem isolates security functions from nonsecurity functions.

Supplemental Guidance: The information subsystem isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information subsystems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk, and address space protections that protect executing code. Information subsystems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception. Related controls: AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	Assessed Status:	

SC-4 Information in Shared Resources

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information subsystems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information subsystems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SC-5 Denial of Service Protection

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The information subsystem protects against or limits the effects of the following types of denial of service attacks: [*(i) "flooding" a network such that legitimate network traffic is prevented or degraded; (ii) disrupting connections between machines such that access to a service is prevented or degraded; (iii) preventing individuals from accessing a service; (iv) disrupting service to systems or persons; (v) Forged User Datagram Protocol (UDP) packets; and (vi) Transmission Control Protocol (TCP) / Internet Control Message Protocol (ICMP) echo request/reply*] by employing [*boundary protection devices in accordance with the requirements specified in CSO-STD-4000, "Network Infrastructure Standard"*].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information subsystem components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. Related controls: SC-6, SC-7.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SC-7 Boundary Protection

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The information subsystem:

a. monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b. implements subnetworks for publicly accessible system components that are [*physically or logically*] separated from internal organizational networks; and

c. connects to external networks or information subsystems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information subsystems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 3: Boundary Protection | Access Points

The organization limits the number of external network connections to the information subsystem.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.

Control Enhancement 3 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 4: Boundary Protection | External Telecommunications Services

The organization:

a. implements a managed interface for each external telecommunication service;

b. establishes a traffic flow policy for each managed interface;

c. protects the confidentiality and integrity of the information being transmitted across each interface;

d. documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

e. reviews exceptions to the traffic flow policy [(*i) at least annually for Low sensitivity systems; (ii) at least annually for Moderate sensitivity systems; or (iii) at least semi-annually (i.e., every six months) for High sensitivity systems*] and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance: Related control: SC-8.

Control Enhancement 4 Implementation Detail	Assessed Status:	

Control Type:	Hybrid

Control Enhancement 5: Boundary Protection | Deny By Default / Allow By Exception

The information subsystem at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

Control Enhancement 5 Implementation Detail	Assessed Status:	

Control Type:	Hybrid

Control Enhancement 7: Boundary Protection | Prevent Split Tunneling for Remote Devices

The information subsystem, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Supplemental Guidance: This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information subsystem by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information subsystem resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

Control Enhancement 7 Implementation Detail	Assessed Status:	

Control Type:	Hybrid

Control Enhancement 8: Boundary Protection | Route Traffic to Authenticated Proxy Servers

The information subsystem routes [*web traffic (i.e., all HTTP/ HTTP Security [HTTPS] communications traffic) originating from NRC systems*] to [*all external networks*] through authenticated proxy servers at managed interfaces.

Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., information subsystem or application) that acts as an intermediary for clients requesting information subsystem resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.

Control Enhancement 8 Implementation Detail	Assessed Status:	

Control Type:	Hybrid

Control Enhancement 18: Boundary Protection | Fail Secure

The information subsystem fails securely in the event of an operational failure of a boundary protection device.

Supplemental Guidance: Fail secure is a condition achieved by employing information subsystem mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information subsystems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases. Related controls: CP-2, SC-24.		
Control Enhancement 18 Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 21: Boundary Protection | Isolation of Information subsystem Components The organization employs boundary protection mechanisms to separate [*information subsystem components*] supporting [*mission or business functions such as: (i) network management components supporting security-related functions; (ii) components within a system authorized to store and/or process different levels of plaintext information. This includes publicly available, non-public/non-sensitive, and/or Sensitive Unclassified Non-safeguards Information (SUNSI) categorized at different levels (e.g., Low, Moderate, High); (iii) research and development components from production components; and (iv) guest components from production components*]. Supplemental Guidance: Organizations can isolate information subsystem components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber-attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys. Related controls: CA-9, SC-3.		
Control Enhancement 21 Implementation Detail	**Assessed Status:**	

SC-8 Transmission Confidentiality and Integrity

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**System-Specific**	
Main Control: The information subsystem protects the [*confidentiality and integrity*] of transmitted information. Supplemental Guidance: This control applies to both internal and external networks and all types of information subsystem components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4. References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; CNSS Policy 15; NSTISSI No. 7003.		

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**
Control Enhancement 1: Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection The information subsystem implements cryptographic mechanisms to [*prevent unauthorized disclosure of information and to detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards such as keeping transmission within physical areas (e.g., cages, data centers, facilities) rated in accordance with the sensitivity of the information*]. Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.	

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

SC-10 Network Disconnect

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**
Main Control: The information subsystem terminates the network connection associated with a communications session at the end of the session or after [*no more than 15 minutes*] of inactivity. Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses. Control Enhancements: None. References: None.		

Main Control Implementation Detail	**Assessed Status:**	

SC-12 Cryptographic Key Establishment and Management

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**
Main Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information subsystem in accordance with [*CSO-STD-2009*]. Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to		

organizational information subsystems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17. References: NIST Special Publications 800-56, 800-57.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**System-Specific**	
Control Enhancement 1: Cryptographic Key Establishment and Management | Availability The organization maintains availability of information in the event of the loss of cryptographic keys by users. Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

SC-13 Cryptographic Protection

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**System-Specific**	
Main Control: The information subsystem implements [*NIST FIPS 140-2 validated cryptography to protect controlled unclassified information, digital signatures, random number generation, and hash generation*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7. Control Enhancements: None. References: FIPS Publication 140-2; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov.		
Main Control Implementation Detail	**Assessed Status:**	

SC-15 Collaborative Computing Devices

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:	**System-Specific**	
Main Control: The information subsystem: a. prohibits remote activation of collaborative computing devices with the following exceptions: [*(i) when necessary for a video teleconferencing (VTC) operator to activate conferencing systems in different rooms where an explicit indication of use to the local users (e.g., use of a camera or microphone) is provided; and (ii) NRC DAA authorized remote activation implementations*]; and		

b. provides an explicit indication of use to users physically present at the devices. Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated. Related control: AC-21. Control Enhancements: None. References: None.

Main Control Implementation Detail	Assessed Status:	

SC-17 Public Key Infrastructure Certificates

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization issues public key certificates [*in accordance with CSO-STD-2009*] or obtains public key certificates from an approved service provider.

Supplemental Guidance: For all certificates, organizations manage information subsystem trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information subsystems and certificates related to the internal operations of systems, for example, application-specific time services. Related control: SC-12.

Control Enhancements: None.

References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.

Main Control Implementation Detail	Assessed Status:	

SC-18 Mobile Code

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. defines acceptable and unacceptable mobile code and mobile code technologies;

b. establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. authorizes, monitors, and controls the use of mobile code within the information subsystem.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information subsystems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information subsystems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.

Control Enhancements: None.

References: NIST Special Publication 800-28; DoD Instruction 8552.01.

Main Control Implementation Detail	Assessed Status:	

SC-19 Voice over Internet Protocol

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information subsystem if used maliciously; and

b. authorizes, monitors, and controls the use of VoIP within the information subsystem.

Supplemental Guidance: Related controls: CM-6, SC-7, SC-15.

Control Enhancements: None.

References: NIST Special Publication 800-58.

Main Control Implementation Detail	Assessed Status:	

SC-20 Secure Name / Address Resolution Service (Authoritative Source)

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The information subsystem:

a. provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Supplemental Guidance: This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information subsystems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information subsystems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Control Enhancements: None.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

Main Control Implementation Detail	Assessed Status:	

SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The information subsystem requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Supplemental Guidance: Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information subsystems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information subsystems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data. Related controls: SC-20, SC-22.

Control Enhancements: None.

References: NIST Special Publication 800-81.

Main Control Implementation Detail	**Assessed Status:**	

SC-22 Architecture and Provisioning For Name / Address Resolution Service

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The information subsystems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance: Information subsystems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists). Related controls: SC-2, SC-20, SC-21, SC-24.

Control Enhancements: None.

References: NIST Special Publication 800-81.

Main Control Implementation Detail	**Assessed Status:**	

SC-23 Session Authenticity

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem protects the authenticity of communications sessions.

Supplemental Guidance: This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. Related controls: SC-8, SC-10, SC-11.

Control Enhancements: None.

References: NIST Special Publications 800-52, 800-77, 800-95.

Main Control Implementation Detail	**Assessed Status:**	

SC-24 Fail in Known State

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization ensures the [*system contingency plan defines known system failure states (e.g., safe mode, recovery mode, fail open/fail closed) for each type of failure*] preserving [*system state information (e.g., system logs)*] in failure.

Supplemental Guidance: Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information subsystems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information subsystem state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes. Related controls: CP-2, CP-10, CP-12, SC-7, SC-22.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SC-28 Protection of Information at Rest

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem protects the [*confidentiality and integrity*] of [*SUNSI and SGI at rest in accordance with CSO-STD-2004*].

Supplemental Guidance: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information subsystems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve

confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7. Control Enhancements: None. References: NIST Special Publications 800-56, 800-57, 800-111.

Main Control Implementation Detail	**Assessed Status:**	

SC-39 Process Isolation

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem maintains a separate execution domain for each executing process.

Supplemental Guidance: Information subsystems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information subsystem process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies. Related controls: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SE-1 Inventory of Personally Identifiable Information

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. establishes, maintains, and updates [*at least every 2 years*] an inventory that contains a listing of all programs and information subsystems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and

b. provides each update of the PII inventory to the CIO or information security official [*at least every 2 years*] to support the establishment of information security requirements for all new or modified information subsystems containing PII.

Supplemental Guidance: The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, organizations may extract the following information elements from Privacy Impact Assessments (PIA) for information subsystems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information subsystem; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII. Related controls: AR-1, AR-4, AR-5, AT-1, DM-1, PM-5.

Control Enhancements: None. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22; OMB Circular A-130, Appendix I; FIPS Publication 199; NIST Special Publications 800-37, 800-122.		
Main Control Implementation Detail	**Assessed Status:**	

SE-2 Privacy Incident Response

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**

Main Control: The organization:

a. develops and implements a Privacy Incident Response Plan; and

b. provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Supplemental Guidance: In contrast to the Incident Response (IR) family in Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the SAOP/CPO. The plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), consistent with organizational incident management structures; and (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach. Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate. Related controls: AR-1, AR-4, AR-5, AR-6, AU-1 through 14, IR-1 through IR-8, RA-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 06-19, 07-16; NIST Special Publication 800-37.

Main Control Implementation Detail	**Assessed Status:**	

SI-1 System and Information Integrity Policy and Procedures

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. develops, documents, and disseminates to [*CIO; CISO; Designated Accrediting Authority (DAA); IT executive; IT manager; IT functional manager; IT systems development official; IT auditor; system owners; ISSOs; system administrators (e.g., database, network); office ISSOs*]: (i) a system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. reviews and updates [*as needed*] the current: (i) system and information integrity policy [*at least annually*]; and

system and information integrity procedures [*at least annually*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information subsystems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Main Control Implementation Detail	**Assessed Status:**	

SI-2 Flaw Remediation

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. identifies, reports, and corrects information subsystem flaws;

b. tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. installs security-relevant software and firmware updates within [*(i) 30 calendar days of the vendor's release of updates of critical importance; (ii) 45 calendar days of the vendor's release of updates of high importance; (iii) 60 calendar days of the vendor's release of updates of moderate importance; and (iv) 90 calendar days of the vendor's release of updates of low importance*]; and

d. incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: Organizations identify information subsystems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information subsystems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information subsystem or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

References: NIST Special Publications 800-40, 800-128.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**	
Control Enhancement 1: Flaw Remediation | Central Management The organization centrally manages the flaw remediation process. Supplemental Guidance: Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**	
Control Enhancement 2: Flaw Remediation | Automated Flaw Remediation Status The organization employs automated mechanisms [*(i) at least quarterly for Low sensitivity systems; (ii) at least quarterly for Moderate sensitivity systems; or (iii) at least monthly for High sensitivity systems*] to determine the state of information subsystem components with regard to flaw remediation. Supplemental Guidance: Related controls: CM-6, SI-4.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	

SI-3 Malicious Code Protection

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. employs malicious code protection mechanisms at information subsystem entry and exit points to detect and eradicate malicious code;

b. updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. configures malicious code protection mechanisms to: (i) perform periodic scans of the information subsystem [*in accordance with CSO-STD-2108, "Endpoint Protection Security Standard"*] and real-time scans of files from external sources at [*endpoints and network entry and exit points as the files are downloaded, opened, or executed in accordance with CSO-STD-2108*]; and (ii) [*performs the actions specified in CSO-STD-2108*] in response to malicious code detection; and

d. addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information subsystem.

Supplemental Guidance: Information subsystem entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information subsystem vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the

detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. References: NIST Special Publications 800-83.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 1: Malicious Code Protection | Central Management The organization centrally manages malicious code protection mechanisms. Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	
Control Type:	**Hybrid**	
Control Enhancement 2: Malicious Code Protection | Automatic Updates The information subsystem automatically updates malicious code protection mechanisms. Supplemental Guidance: Malicious code protection mechanisms include, for example, signature definitions. Due to information subsystem integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.		
Control Enhancement 2 Implementation Detail	**Assessed Status:**	

SI-4 Information subsystem Monitoring

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization:

a. monitors the information subsystem to detect: (i) attacks and indicators of potential attacks in accordance with [*NRC policy, standards, processes, procedures, and checklists issued by the CSO*]; and (ii) unauthorized local, network, and remote connections;

b. identifies unauthorized use of the information subsystem through [*the use of computer system monitoring methods in accordance with CSO-STD-2005*];

c. deploys monitoring devices: (i) strategically within the information subsystem to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. heightens the level of information subsystem monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. obtains legal opinion with regard to information subsystem monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g. provides [*information subsystem monitoring records, such as reports and alerts*] to the [*system ISSO*] on a [*daily basis*].

Supplemental Guidance: Information subsystem monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information subsystem boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information subsystem. Organizations can monitor information subsystems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information subsystem monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information subsystems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information subsystem monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Information subsystem Monitoring | Automated Tools for Real-Time Analysis

The organization employs automated tools to support near real-time analysis of events.

Supplemental Guidance: Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information subsystems.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 4: Information subsystem Monitoring | Inbound and Outbound Communications Traffic

The information subsystem monitors inbound and outbound communications traffic [*on a real-time basis*] for unusual or unauthorized activities or conditions.

Supplemental Guidance: Unusual/unauthorized activities or conditions related to information subsystem inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information subsystems or propagating among system components, the unauthorized exporting of information, or signaling to external information subsystems. Evidence of malicious code is used to identify potentially compromised information subsystems or information subsystem components.

Control Enhancement 4 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 5: Information subsystem Monitoring | System-Generated Alerts

The information subsystem alerts the [*system administrator; system ISSO; Security Operations Center (SOC); and CSIRT*] when the following indications of compromise or potential compromise occur: [*(i) malicious code detection; (ii) spear-phishing attempts; (iii) attempted or actual egress of large quantities of data to known or suspected malicious and unauthorized Internet Protocol addresses; (iv) attempted or actual unauthorized internal scans and/or probes of the infrastructure; (v) attempted or actual spam from internal email addresses; or (vi) if a device's security is*

compromised]. Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information subsystem security officers. Related controls: AU-5, PE-6.

Control Enhancement 5 Implementation Detail	**Assessed Status:**	

SI-5 Security Alerts, Advisories, and Directives

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**<Common>**

Main Control: The organization:

a. receives information subsystem security alerts, advisories, and directives from the [*US-CERT, and other external organizations (e.g., Law Enforcement)*] on an ongoing basis;

b. generates internal security alerts, advisories, and directives as deemed necessary;

c. disseminates security alerts, advisories, and directives to: [*to system owners, ISSOs, and system administrators*]; and

d. implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.

References: NIST Special Publication 800-40.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**<Common>**

Control Enhancement 1: Security Alerts, Advisories, and Directives | Automated Alerts and Advisories

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

Supplemental Guidance: The significant number of changes to organizational information subsystems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk including the governance level, mission/business process/enterprise architecture level, and the information subsystem level.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

SI-6 Security Function Verification

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem:

a. verifies the correct operation of [*all security functions*];

b. performs this verification [*at least quarterly*];

c. notifies the [*system administrator and system ISSO*] of failed security verification tests; and

d. [*shuts the information subsystem down, restarts the information subsystem, or restores the affected security functions within the system to a known secure state*] when anomalies are discovered.

Supplemental Guidance: Transitional states for information subsystems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information subsystems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SI-7 Software, Firmware, and Information Integrity

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The organization employs integrity verification tools to detect unauthorized changes to [*software and any information that is stored, processed, or transmitted by the system*].

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information subsystems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.

References: NIST Special Publications 800-147, 800-155.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Software, Firmware, and Information Integrity | Integrity Checks

The information subsystem performs an integrity check of [*software and information in accordance with CSO-STD-2108*].

Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information subsystems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 2: Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations

The organization employs automated tools that provide notification to [*system administrators and system ISSOs*] upon discovering discrepancies during integrity verification.

Supplemental Guidance: The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business owners, information subsystem owners, systems administrators, software developers, systems integrators, and information security officers.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 5: Software, Firmware, and Information Integrity | Automated Response to Integrity Violations

The information subsystem automatically [*notifies the system administrator and system ISSO*] when integrity violations are discovered.

Supplemental Guidance: Organizations may define different integrity checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within organizational information subsystems includes, for example, reversing the changes, halting the information subsystem, or triggering audit alerts when unauthorized modifications to critical security files occur.

Control Enhancement 5 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 7: Software, Firmware, and Information Integrity | Integration of Detection and Response

The organization incorporates the detection of unauthorized [*changes to established configuration settings*] into the organizational incident response capability.

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information subsystem privileges. Related controls: IR-4, IR-5, SI-4.

Control Enhancement 7 Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 14: Software, Firmware, and Information Integrity | Binary or Machine Executable Code

The organization:

a. prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and

b. provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts.

The assessments address the fact that these types of software products may be very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations. Related control: SA-5.		
Control Enhancement 14 Implementation Detail	**Assessed Status:**	

SI-8 Spam Protection

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**Hybrid**

Main Control: The organization:

a. employs spam protection mechanisms at information subsystem entry and exit points to detect and take action on unsolicited messages; and

b. updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental Guidance: Information subsystem entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.

References: NIST Special Publication 800-45.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 1: Spam Protection | Central Management

The organization centrally manages spam protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

Control Type:	**Hybrid**

Control Enhancement 2: Spam Protection | Automatic Updates

The information subsystem automatically updates spam protection mechanisms.

Supplemental Guidance: None.

Control Enhancement 2 Implementation Detail	**Assessed Status:**	

SI-10 Information Input Validation

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem checks the validity of [*all information subsystem inputs to web/application servers, database servers, and any system or application input that might receive a crafted exploit toward executing some code or buffer overflow*].

Supplemental Guidance: Checking the valid syntax and semantics of information subsystem inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SI-11 Error Handling

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem:

a. generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

b. reveals error messages only to [*systems owners, system ISSOs, and system administrators*].

Supplemental Guidance: Organizations carefully consider the structure/content of error messages. The extent to which information subsystems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SI-12 Information Handling and Retention

Implementation Priority:	P2	This control relies on functionality provided by P1 controls, and provides functionality required for P3 controls. It should be implemented after all P1 controls and before any P3 controls.
Control Type:		**System-Specific**

Main Control: The organization handles and retains information within the information subsystem and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information subsystems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

SI-16 Memory Protection

Implementation Priority:	P1	This is a foundational control and should be implemented before any P2 or P3 controls.
Control Type:		**System-Specific**

Main Control: The information subsystem implements [*memory protections that prevent the execution of code stored in non-executable regions of memory or in prohibited memory locations using hardware or software data execution prevention (DEP) safeguards*] to protect its memory from unauthorized code execution.

Supplemental Guidance: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3.

Control Enhancements: None.

References: None.

Main Control Implementation Detail	**Assessed Status:**	

TR-1 Privacy Notice

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

b. describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific

uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and

c. revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Supplemental Guidance: Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE).124 Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel. Related controls: AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16, 10-22, 10-23; ISE Privacy Guidelines.

Main Control Implementation Detail	**Assessed Status:**	

Control Type:	**System-Specific**

Control Enhancement 1: Privacy Notice | Real-Time or Layered Notice

The organization provides real-time and/or layered notice when it collects PII.

Supplemental Guidance: Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed/specific information.

Control Enhancement 1 Implementation Detail	**Assessed Status:**	

TR-2 System of Records Notices and Privacy Act Statements

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);

b. keeps SORNs current; and

c. includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Supplemental Guidance: Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for

example, when conducting telephone interviews or surveys). Related control: DI-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130.		
Main Control Implementation Detail	**Assessed Status:**	
Control Type:	**<Common>**	
Control Enhancement 1: System of Records Notices and Privacy Act Statement | Public Website Publication The organization publishes SORNs on its public website. Supplemental Guidance: None.		
Control Enhancement 1 Implementation Detail	**Assessed Status:**	

TR-3 System of Records Notices and Privacy Act Statements

Implementation Priority:	N/A	N/A
Control Type:		**<Common>**
Main Control: The organization: a. ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and b. ensures that its privacy practices are publicly available through organizational websites or otherwise. Supplemental Guidance: Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices. Related control: AR-6. Control Enhancements: None. References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-23.		
Main Control Implementation Detail	**Assessed Status:**	

UL-1 Internal Use

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**
Main Control: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices. Supplemental Guidance: Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII. Related controls: AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2. Control Enhancements: None.		

References: The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1).		
Main Control Implementation Detail	**Assessed Status:**	

UL-2 Information Sharing with Third Parties

Implementation Priority:	N/A	N/A
Control Type:		**Hybrid**

Main Control: The organization:

a. shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;

b. where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;

c. monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and

d. evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Supplemental Guidance: The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared. Related controls: AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines.

Main Control Implementation Detail	**Assessed Status:**	