Nuclear Regulatory Commission
Computer Security Office
Computer Security Standard

Office Instruction:	**CSO-STD-0021**
Office Instruction Title:	**Common and Hybrid Security Control Standard**
Revision Number:	**1.0**
Issuance Date:	**Date of last signature**
Effective Date:	**September 1, 2015**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PCT**
Summary of Changes:	CSO-STD-0021, "Common and Hybrid Security Control Standard," provides the Nuclear Regulatory Commission (NRC) with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, common and hybrid security controls required for NRC systems processing information up to, and including, the Safeguards Information (SGI) level.
Training:	Upon Request
ADAMS Accession No.:	ML15210A417

Approvals				
Primary Office Owner	Policy, Compliance, and Training		**Signature**	**Date**
Standards Working Group Chair	Bill Dabbs		**/RA/**	**8/4/15**
Responsible SITSO	Kathy Lyons-Burke		**/RA/**	**8/4/15**
DAA for Non-Major IT Investments	Director, CSO	Tom Rich	**/RA/**	**8/4/15**
	Director, OIS	Jim Flanagan	**/RA/**	**8/5/15**

TABLE OF CONTENTS

List of Tables

Computer Security Standard

CSO-STD-0021

Common and Hybrid Security Control Standard

---

1 PURPOSE

CSO-STD-0021, "Common and Hybrid Security Control Standard," provides the Nuclear Regulatory Commission (NRC) with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," common and hybrid security controls required for NRC systems processing information up to, and including, the Safeguards Information (SGI) level. In addition, this standard identifies the common and hybrid security control providers and defines their responsibilities for the common and hybrid security controls.

This standard is for common and hybrid security control providers, system owners, and information system security officers (ISSOs) who have the required knowledge, skill, and ability to develop, apply, enforce, and monitor the security requirements.

This standard identifies but does **not** define system-specific security controls.

2 INTRODUCTION

The security requirements specified in this standard relate to the secure implementation and maintenance of the common and hybrid security controls. This section introduces the types of security controls to be implemented and the providers responsible for the security controls.

2.1 Security Control Types

There are three distinct types of security controls that define the scope of applicability for the security control, the shared nature of the control, and the responsibility for control implementation:

- Common Security Control: A security control that is implemented at the NRC level and fulfilled for all NRC systems regardless of location. Because common security controls protect multiple organizational systems of differing impact levels, the controls are implemented with regard to the highest impact level among the systems.
- Hybrid Security Control: A security control that is implemented for an NRC system in part as a common security control (or inherited from another source, such as another NRC office or system) and in part as a system-specific security control.
- System-Specific Security Control: A security control implemented for a system that has not been designated by the NRC as a common control, and is not provided by another system as an inherited control. System-specific security controls are the primary

responsibility of system owners. These controls are identified within the security control tables in Section 4, Specific Requirements, but are grayed out because they are not the focus of this standard.

In addition to the security control types described above, the Federal Information Security Management Act (FISMA) requires organizations to develop and implement an organization-wide information security program to address information security for the systems that support the operations and assets of the organization. The information security program management (PM) controls are implemented at the NRC level and are not directed at the individual system. These PM controls complement the system security controls but focus on the programmatic, NRC-wide information security requirements that are independent of any particular system and are considered to be common security controls.

2.2 Common Security Control Provider

Managing system-related security risks is a complex effort that requires the involvement of the entire organization—from senior executives providing the supervision, guidance, and direction, to office directors, planning and managing security for NRC systems owned by their office, to individuals on the front lines developing, implementing, and operating the systems supporting the NRC's core missions and business processes. The common security control providers are office directors or regional administrators with responsibility for specific types of NRC-wide security controls. They are responsible for the development, implementation, assessment, and monitoring of specific common security controls and are held accountable for the security risk associated with operating the common security controls.

2.3 Hybrid Security Control Responsibilities

Hybrid security controls are controls that are partially provided at the NRC level and partially provided at the system level. For the portion of a hybrid security control that is system-specific, the responsibilities are entrusted with the system owner.

The NRC system owner has the overall responsibility for the security, procurement, development, integration, modification, operation, maintenance, and disposal of an NRC system operated by or on behalf of NRC. Additionally, the NRC system owner has the responsibility for ensuring that security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements for NRC systems hosted in non-NRC facilities.

3 GENERAL REQUIREMENTS

This section addresses the general requirements that common and hybrid security control providers, system owners, and ISSOs responsible for implementing security controls must comply with as the minimum set of controls.

This standard must be used in conjunction with:

- CSO-STD-0020, "Organization Defined Values for System Security Controls." This standard defines the required NRC values for specific computer security controls identified in federal computer security control standards and guidance. System owners

must use this standard to ensure the information system security controls are in compliance with the required NRC values.

3.1 Common and Hybrid Security Control Providers

Common and hybrid security control providers must:

- Ensure that all entities within their organization and/or under their control comply with NRC security authorization requirements and that required security documentation is prepared and maintained for each common and hybrid security control.
- Keep control status current.
- Inform system owners of significant changes in common and hybrid security controls that may impact system-specific security control implementation.
- Inform system owners when problems arise with a common or hybrid security control (e.g., when an annual security assessment indicates the control is flawed or deficient in some manner) that renders the security control less effective.

4 SPECIFIC REQUIREMENTS

This section provides specific requirements for security controls, including identifying common and hybrid security controls and the common and hybrid security control provider responsibilities for each control family. In addition, this section defines the circumstances that would exempt a system from inheriting a common or hybrid security control.

Table 4-1 lists the security control families identified in NIST SP 800-53, Revision 4, and the order in which they are addressed in this section.

Table 4-1: Security Control Identifiers and Family Names

ID	Control Family Name	ID	Control Family Name
Assurance-Related Controls			
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance		
Program Management Controls			
PM	Program Management		
Privacy Controls			

ID	Control Family Name	ID	Control Family Name
AP	Authority and Purpose	IP	Individual Participation and Redress
AR	Accountability, Audit, and Risk Management	SE	Security
DI	Data Quality and Integrity	TR	Transparency
DM	Data Minimization and Retention	UL	Use Limitation

4.1 Assurance-Related Controls

Security assurance is a critical aspect in determining the trustworthiness of information systems. Assurance is the measure of confidence that the security functions, features, practices, policies, procedures, mechanisms, and architecture of NRC systems accurately mediate and enforce established security policies.

4.1.1 Access Control Policy and Procedures

Table 4.1-1 summarizes the common and hybrid security control responsibilities for the AC family. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-1: AC Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
AC-1	Access Control Policy and Procedures	Computer Security Office (CSO), System Owners	Hybrid
AC-2	Account Management	CSO, Office of Information Services (OIS), System Owners	Hybrid
AC-2[1]	Automated System Account Management	System Owners	System Specific
AC-2[2]	Removal of Temporary / Emergency Accounts	System Owners	System Specific
AC-2[3]	Disable Inactive Accounts	CSO, OIS, System Owners	Hybrid
AC-2[4]	Automated Audit Actions	System Owners	System Specific
AC-2[5]	Inactivity Logout	CSO, OIS, System Owners	Hybrid
AC-2[11]	Usage Conditions	System Owners	System Specific
AC-2[12]	Account Monitoring / Atypical Usage	System Owners	System Specific
AC-2[13]	Disable Accounts for High-Risk Individuals	System Owners	System Specific
AC-3	Access Enforcement	System Owners	System Specific
AC-4	Information Flow Enforcement	System Owners	System Specific
AC-5	Separation of Duties	System Owners	System Specific
AC-6	Least Privilege	System Owners	System Specific

Control ID	Control Title	Provider(s)	Control Type
AC-6[1]	Authorized Access to Security Functions	System Owners	System Specific
AC-6[2]	Non-Privileged Access for Nonsecurity Functions	System Owners	System Specific
AC-6[3]	Network Access to Privileged Commands	System Owners	System Specific
AC-6[5]	Privileged Accounts	System Owners	System Specific
AC-6[9]	Auditing Use of Privileged Functions	System Owners	System Specific
AC-6[10]	Prohibit Non-privileged Users from Executing Privileged Functions	System Owners	System Specific
AC-7	Unsuccessful Logon Attempts	System Owners	System Specific
AC-8	System Use Notification	CSO, OIS, System Owners	Hybrid
AC-10	Concurrent Session Control	System Owners	System Specific
AC-11	Session Lock	CSO, OIS, System Owners	Hybrid
AC-11[1]	Pattern-Hiding Displays	OIS, System Owners	Hybrid
AC-12	Session Termination	System Owners	System Specific
AC-14	Permitted Actions without Identification or Authentication	System Owners	System Specific
AC-17	Remote Access	CSO, OIS, System Owners	Hybrid
AC-17[1]	Automated Monitoring / Control	OIS, System Owners	Hybrid
AC-17[2]	Protection of Confidentiality / Integrity Using Encryption	CSO, OIS, System Owners	Hybrid
AC-17[3]	Managed Access Control Points	OIS, System Owners	Hybrid
AC-17[4]	Privileged Commands / Access	System Owners	System Specific
AC-18	Wireless Access	CSO, OIS, System Owners	Hybrid
AC-18[1]	Authentication and Encryption	System Owners	System Specific
AC-18[4]	Restrict Configurations by Users	System Owners	System Specific
AC-18[5]	Antennas / Transmission Power Levels	System Owners	System Specific
AC-19	Access Control for Mobile Devices	CSO, OIS, System Owners	Hybrid
AC-19[5]	Full Device / Container-Based Encryption	System Owners	System Specific
AC-20	Use of External Information Systems	Office of the Executive Director for Operations (OEDO), CIO, CSO, System Owners	Hybrid
AC-20[1]	Limits on Authorized Use	System Owners	System Specific
AC-20[2]	Portable Storage Devices	CSO, System Owners	Hybrid

Control ID	Control Title	Provider(s)	Control Type
AC-21	Information Sharing	System Owners	System Specific
AC-22	Publicly Accessible Content	System Owners	System Specific

4.1.1.1 AC-1 Access Control Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles:
  - An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the access control policy and associated access controls;
- Reviews and updates the current:
  - Access control policy within the NRC-defined frequency; and
  - Access control procedures within the NRC-defined frequency.

Provider Responsibilities:

CSO must:

- Develop, document, and review/update agency-wide access control policy, define the frequency for reviews and updates, define organization–defined values, and distribute to NRC users.

System owners must:

- Ensure system-specific access control procedures are developed, reviewed/updated, and maintained for the systems in accordance with NRC requirements.
- Ensure that system-specific access control procedures facilitate the implementation of access control policy.

4.1.1.2 AC-2 Account Management

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Identifies and selects the types of information system accounts to support organizational missions/business functions as defined in CSO-STD-0020;
- Assigns account managers for information system accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of the information system, group and role membership, access authorizations (i.e., privileges), and other attributes (as required) for each account;
- Requires approvals by NRC-defined personnel or roles for requests to create information system accounts;
- Creates, enables, modifies, disables, and removes information system accounts in accordance with CSO-STD-0020 and including but not limited to other NRC requirements;
- Monitors the use of information system accounts;
- Notifies account managers:
  - When accounts are no longer required;
  - When users are terminated, transferred, or suspended; and
  - When individual information system usage or need-to-know changes;
- Authorizes access to the information system based on:
  - A valid access authorization;
  - Intended system usage; and
  - Other attributes as required by the organization or associated mission/business functions;
- Reviews accounts for compliance with account management requirements in accordance with CSO-STD-0020 and other NRC requirements; and
- Establishes a process for reissuing group account credentials (if deployed) when individuals are removed from the group.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide account management policy, and distribute to NRC users.

OIS must**:**

- Provide limited account management functions for those systems that implement the Enterprise Single Sign-On (ESSO) solution and have been previously approved for access into the application. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session. The user must be on the NRC network, either directly through the Local Area Network (LAN) connection, or remotely through a Citrix®[1] remote access connection or Virtual Private Network (VPN) connection.

System owners must:

- Assign account manager for system accounts and establish conditions for group and role membership.
- Notify account managers:
  - When accounts are no longer required;
  - When users are terminated or transferred; and
  - When individual information system usage or need-to-know changes.
- Ensure the user has been approved for access into the application and has the appropriate rights/permissions based on a valid need-to-know.
- Monitor and review accounts in accordance with CSO-STD-0020 and other NRC requirements.
- For systems on the NRC internal network, notify OIS when access should be terminated.
- Systems that are not integrated with NRC's Active Directory (AD) for single sign-on must create, enable, modify, audit, disable, and remove information system accounts in accordance with CSO-STD-0020 and other NRC requirements.
- For systems on another network, notify the network owner when access should be terminated.

4.1.1.2.1 AC-2[3] Disable Inactive Accounts

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The system ISSO ensures the information system automatically disables inactive accounts in accordance with CSO-STD-0020 and other NRC requirements.

[1] Citrix® is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries."

Provider Responsibilities:

CSO must:

- Define the timeframe for automatically disabling inactive accounts.

OIS must:

- Ensure the NRC user account is disabled in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Disable accounts under the system owner's control.
- For systems on the NRC managed network, notify OIS when account should be disabled.
- For systems on another network, notify the network owner when an account should be disabled.

4.1.1.2.2 AC-2[5] Inactivity Logout

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The system owner ensures the information system logs users out in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define the time period of inactivity before the information system logs out the user.

OIS must:

- Dissconnect inactive sessions for the NRC desktop/laptop in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that the application inactive session related controls are configured in accordance with CSO-STD-0020 and other NRC requirements.

4.1.1.3 AC-8 System Use Notification

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- 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:
  - Users are accessing a U.S. Government information system;
  - Information system usage may be monitored, recorded, and subject to audit;
  - Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
  - Use of the information system indicates consent to monitoring and recording;
- 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 system; and
- For publicly accessible systems:
  - Displays system use information notification message/banner in accordance with CSO-STD-0040 before granting further access;
  - Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
  - Includes a description of the authorized uses of the system.

Provider Responsibilities:

CSO must:

- Provide policy and requirements for the NRC-approved system use notification.

OIS must:

- Provide the NRC-approved system use notification for Windows components connected to the enterprise NRC domain. The enterprise NRC domain refers to the Microsoft Active Directory domain at NRC which Windows servers and workstations are connected to and managed through. For all other devices, the NRC-approved system use notification must be set locally.

System owners must:

- Ensure the NRC-approved system use notification is displayed in accordance with CSO-STD-0040 before granting access to the system.

4.1.1.4 AC-11 Session Lock

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The information system:

- Prevents further access to the system by initiating a session lock in accordance with CSO-STD-0020 and other NRC requirements; and
- Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Provider Responsibilities:

CSO must:

- Establish requirements for session lock.

OIS must:

- Ensure session lock for Windows components connected to the enterprise NRC domain is provided. For all other devices, session lock must be provided in accordance with NRC requirements.

System owners must:

- Ensure session lock is provided in accordance with CSO-STD-0020 and other NRC requirements.

4.1.1.4.1 AC-11[1] Pattern-Hiding Displays

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Provider Responsibilities:

OIS must:

- Conceal, via session lock for Windows components connected to the enterprise NRC domain, information previously visible on the display with a publicly viewable image. For all other components, session lock must be provided in accordance with NRC requirements.

System owners must:

- Ensure session lock conceals information previously visible on the display with a publicly viewable image in accordance with NRC requirements.

4.1.1.5 AC-17 Remote Access

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
- Authorizes remote access to the information system prior to allowing such connections.

Provider Responsibilities:

CSO must:

- Provide agency-wide usage restrictions, configuration requirements, and implementation requirements for remote access. Security requirements for remote access to NRC systems processing information up to, and including, the Sensitive Unclassified Non-Safeguards Information (SUNSI) level are provided within CSO-STD-2105, “Remote Access Security Standard.”

OIS must:

- Provide remote access methods (e.g., Citrix, VPN) to remotely access NRC systems connected to the enterprise NRC domain.

System owners must:

- Ensure the system is compliant with agency-wide usage restrictions, configuration requirements, and implementation requirements for remote access.
- Authorize remote access to the information system prior to allowing such connections.
- Ensure that systems not connected to the domain are routed through Trusted Internet Connections as defined in CSO-STD-0020.

4.1.1.5.1 AC-17[1] Automated Monitoring / Control

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC monitors and controls remote access methods.

Provider Responsibilities:

OIS must:

- Provide automated monitoring and control of remote access methods (e.g., Citrix, VPN) for NRC systems connected to the enterprise NRC domain.

System owners must:

- Ensure that applications providing remote access methods through non-NRC controlled networks monitor and control remote access sessions in accordance with NRC requirements.

4.1.1.5.2 AC-17[2] Protection of Confidentiality / Integrity Using Encryption

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Provider Responsibilities:

CSO must:

- Define the standard for cryptographic controls.

OIS must:

- Provide cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions (e.g., Citrix, VPN) for NRC systems connected to the enterprise NRC domain in accordance with CSO-STD-2009, “Cryptographic Control Standard.”

System owners must:

- Ensure that applications providing remote access methods through non-NRC controlled networks provide cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions in accordance with CSO-STD-2009.

4.1.1.5.3 AC-17[3] Managed Access Control Points

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC routes all remote accesses through managed network access control points.

Provider Responsibilities:

OIS must:

- Route all remote access for NRC systems connected to the enterprise NRC domain through managed network access control points in accordance with NRC requirements.

System owners must:

- Ensure that systems and applications providing remote access methods through non-NRC controlled networks route all remote access through managed network access control points in accordance with NRC requirements.

4.1.1.6 AC-18 Wireless Access

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
- Authorizes wireless access to the information system prior to allowing such connections.

Provider Responsibilities:

CSO must:

- Provide agency-wide usage restrictions, configuration requirements, and implementation requirements for wireless access.

OIS must:

- Provide wireless access to NRC networks in accordance with NRC policy, standards, and guidelines.
- Provide wireless Internet access for guests of the NRC who wish to use Wi-Fi-enabled personal devices such as, but not limited to, laptops, tablets, or smart phones.
- Issue mobile devices that are pre-configured with wireless access limitations to meet NRC's required security objectives and abide by NRC requirements.

System owners must:

- Provide wireless access authorized by the Designated Approving Authority (DAA) that is not provided as stated above.
- Ensure wireless access to the system is authorized by the DAA.

- Ensure requirements and restrictions for wireless connections to the system are enforced.
- Ensure wireless connections are monitored to detect an unauthorized wireless connection and take appropriate actions if discovered.

4.1.1.7 AC-19 Access Control for Mobile Devices

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for NRC-controlled mobile devices; and
- Authorizes the connection of mobile devices to NRC information systems.

Provider Responsibilities:

CSO must:

- Provide policy, agency-wide usage restrictions, configuration requirements, and implementation requirements for NRC-controlled mobile devices.

OIS must:

- Provide NRC users at NRC facilities access control protections for mobile devices, such as, but limited to, mobile devices, mobile desktops, loaner laptops, and encrypted thumb drives in accordance with NRC requirements.

System owners must:

- Provide access control protections for mobile devices authorized by the DAA that are not provided as stated above.
- Ensure access control requirements for system-specific portable and mobile devices are enforced in accordance with NRC requirements.

4.1.1.8 AC-20 Use of External Information Systems

This is a ***hybrid*** security control with responsibilities for the **OEDO**, **Chief Information Officer (CIO)**, **CSO**, and **system owners**.

Control Description:

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

- Access the NRC information system from the external information systems; and
- Process, store, and/or transmit NRC-controlled information using the external information systems.

NRC Supplemental Information:

NIST SP 800-53 Revision 4 provides the following definition:

"External information systems are information systems or components of information systems 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 security control effectiveness."

Provider Responsibilities:

OEDO must:

- Establish agency-wide policy for formal exchange agreements for external system connections.

CIO must:

- Approve external system connections to NRC systems.

CSO must:

- Establish agency-wide terms, conditions and restrictions allowing authorized individuals to:
  - Access NRC systems from external systems;
  - Access external systems from NRC systems; and
  - Process, store, and/or transmite NRC information using external systems.

System owners must:

- Ensure the external system is authorized for the level of information NRC intends to use with the system.
- Establish formal exchange agreements for external system connections and obtain approval from the CIO for the connection. These documents are required parts of the system authorization decision by the NRC DAA.
- Verify the implementation of required security controls on the external system as specified in the external system's security policy and plan.

4.1.1.8.1 AC-20[2] Portable Storage Devices

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC restricts the use of NRC-controlled portable storage devices by authorized individuals on external information systems.

Provider Responsibilities:

CSO must:

- Establish usage restrictions for the use of NRC-controlled portable storage devices by authorized individuals on external systems.

System owners must:

- Establish system-specific restrictions (i.e., rules of behavior) on the use of NRC-controlled portable storage devices by authorized individuals on external systems when creating the formal exchange agreement and obtain approval from the DAA on established use.
- Ensure restrictions are 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.

4.1.2 Awareness and Training

Table 4.1-2 summarizes the common and hybrid security control responsibilities for the AT family. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-2: **AT Control Family Common and Hybrid Security Control Assignments**

Control ID	Control Title	Provider(s)	Control Type
AT-1	Security Awareness and Training Policy and Procedures	CSO, Office of the Chief Human Capital Officer (OCHCO), System Owners	Hybrid
AT-2	Security Awareness Training	CSO, OCHCO, Office Directors/ Regional Administrators, System Owners	Hybrid
AT-2[2]	Insider Threat	Office of Nuclear Security and Incident Response (NSIR), OCHCO	Common
AT-3	Role-Based Security Training	CSO, OCHCO, System Owners	Hybrid
AT-4	Security Training Records	OCHCO, Office Directors/Regional Administrators, System Owners	Hybrid

4.1.2.1 AT-1 Security Awareness and Training Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OCHCO**, and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles:
  - A security awareness and training policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among organizational entities, and compliance; and
  - Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls;
- Reviews and updates the current:
  - Security awareness and training policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Security awareness and training procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide cybersecurity awareness and training policy, define the frequency for reviews and updates, and distribute to NRC users.

OCHCO must:

- Develop, document, review/update agency-wide awareness and training policy, announce availability of awareness and training to NRC users, and provide the agency-wide awareness and training to NRC users.
- Ensure that agency-wide awareness and training policy and procedures are documented for non-badged contractors supporting electronic process of NRC information in accordance with NRC requirements.

System owners must:

- Ensure that system-specific security awareness and training procedures are developed, reviewed/updated and maintained in accordance with NRC requirements for the system and that NRC users abide by security awareness and training requirements.

- Ensure that system-specific security awareness and training procedures facilitate the implementation of the NRC security awareness and training policy.
- Ensure that system-specific security awareness and training procedures are reviewed and updated in accordance with CSO-STD-0020 and other NRC requirements.
- Ensure that system-specific security awareness and training policy and procedures are documented for non-badged contractors supporting NRC systems in accordance with CSO-STD-0020 and other NRC requirements.

4.1.2.2 AT-2 Security Awareness Training

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OCHCO**, **Office Directors and Regional Administrators**, and **system owners**.

Control Description:

The NRC provides basic security awareness training to all information system users (including managers, senior executives, and contractors):

- As part of initial training for new users;
- When required by system changes; and
- Within the NRC-defined frequency thereafter in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Identify acceptable cybersecurity awareness training courses.
- Provide a cybersecurity briefing for new employees.
- Define the frequency of refresher cybersecurity awareness training.

OCHCO must:

- Provide learning system accounts for all individuals that have access to NRC electronic information.
- Provide agency-wide cybersecurity awareness training within the NRC learning system.
- Ensure that a cybersecurity briefing is included in the initial orientation for new employees.

Office Directors and Regional Administrators must:

- Ensure that staff and contractors that have access to NRC electronic information are identified within the NRC learning system and have required accounts in that system.
- Ensure that staff and contractors complete required cybersecurity awareness training.

System owners must:

- Provide system–specific cybersecurity awareness training (e.g., protection of physical and information assets, handling of sensitive system information, special password protection policies, privacy information protections) to enable the system user to have a solid understanding of system security policy and procedures in their day-to-day responsibilities.

4.1.2.2.1 AT-2[2] Insider Threat

This is a ***common*** security control with responsibilities for **NSIR** and **OCHCO**.

Control Description:

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

Provider Responsibilities:

NSIR must:

- Provide insider threat training for all individuals that have access to NRC electronic information that includes training on recognizing and reporting potential indicators of insider threat.

OCHCO must:

- Provide agency-wide cybersecurity awareness training within the NRC learning system.

4.1.2.3 AT-3 Role-Based Security Training

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OCHCO**, **Office Directors and Regional Administrators**, and **system owners**.

Control Description:

The NRC provides role-based security-related training to personnel with assigned security roles and responsibilities:

- Before authorizing access to the information system or performing assigned duties;
- When required by information system changes; and
- Within the NRC-defined frequency thereafter in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Identify role-based cybersecurity training requirements.
- Provide subject matter expert information for agency-specific role-based cybersecurity training.
- Identify commercial courses that meet role-based cybersecurity requirements.

OCHCO must:

- Provide agency-specific role-based cybersecurity training.

Office Directors and Regional Administrators must:

- Identify staff and contractors with cybersecurity roles.
- Ensure that staff and contractors with cybersecurity roles complete computer security training in accordance with their role prior to assuming the role and at the required intervals.
- Track and report to CSO and OCHCO the required cybersecurity training for those individuals performing cybersecurity roles.

System owners must:

- Ensure staff and contractors with cybersecurity roles meet role-based cybersecurity training requirements before assuming the role.
- Provide system-specific technical vendor/commercial training to their staff with information technology (IT) security roles.
- Ensure that staff with significant cybersecurity responsibilities complete the required role-based cybersecurity training prior to performing assigned duties.

4.1.2.4 AT-4 Security Training Records

This is a ***hybrid*** security control with responsibilities for the **OCHCO**, **Office Directors and Regional Administrators**, and **system owners**.

Control Description:

The NRC:

- Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

- Retains individual training records in accordance with Management Directive (MD) 3.53, "NRC Records and Document Management Program" Handbook 1, "NRC Records Management Program."

Provider Responsibilities:

OCHCO must:

- Document and monitor records of security awareness training for NRC IT users.
- Document and monitor records of role-based cybersecurity training.

Office Directors and Regional Administrators must:

- Ensure that records of security awareness training and role-based security-related training are maintained and monitored to meet requirements of their role(s).
- Notify CSO of system-specific and vendor/commercial training taken by contractors.
- Notify OCHCO of system-specific and vendor/commercial training taken by staff.

System owner must:

- Document, monitor and retain records of system-specific and vendor/commercial training in accordance with CSO-STD-0020 and other NRC requirements.

4.1.3 Audit and Accountability

Table 4.1-3 summarizes the common and hybrid security control responsibilities for the AU family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-3: AU Control Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
AU-1	Audit and Accountability Policy and Procedures	CSO, System Owners	Hybrid
AU-2	Audit Events	CSO, System Owners	Hybrid
AU-2[3]	Reviews and Updates	CSO, System Owners	Hybrid
AU-3	Content of Audit Records	System Owners	System Specific
AU-3[1]	Additional Audit Information	System Owners	System Specific
AU-3[2]	Centralized Management of Planned Audit Record Content	System Owners	System Specific
AU-4	Audit Storage Capacity	System Owners	System Specific
AU-5	Response to Audit Processing Failures	System Owners	System Specific
AU-5[1]	Audit Storage Capacity	System Owners	System Specific
AU-5[2]	Real-Time Alerts	System Owners	System Specific
AU-6	Audit Review, Analysis, and Reporting	System Owners	System Specific

Control ID	Control Title	Provider(s)	Control Type
AU-6[1]	Process Integration	System Owners	System Specific
AU-6[3]	Correlate Audit Repositories	System Owners	System Specific
AU-6[5]	Integration / Scanning and Monitoring Capabilities	System Owners	System Specific
AU-6[6]	Correlation with Physical Monitoring	System Owners	System Specific
AU-7	Audit Reduction and Report Generation	System Owners	System Specific
AU-7[1]	Automatic Processing	System Owners	System Specific
AU-8	Time Stamps	System Owners	System Specific
AU-8[1]	Synchronization with Authoritative Time Source	System Owners	System Specific
AU-9	Protection of Audit Information	System Owners	System Specific
AU-9[2]	Audit Backup on Separate Physical Systems / Components	System Owners	System Specific
AU-9[3]	Cryptographic Protection	System Owners	System Specific
AU-9[4]	Access by Subset of Privileged Users	System Owners	System Specific
AU-10	Non-Repudiation	System Owners	System Specific
AU-11	Audit Record Retention	System Owners	System Specific
AU-12	Audit Generation	System Owners	System Specific
AU-12[1]	System-Wide / Time-Correlated Audit Trail	System Owners	System Specific
AU-12[3]	Changes by Authorized Individuals	System Owners	System Specific

4.1.3.1 AU-1 Audit and Accountability Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - An audit and accountability policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among organizational entities, and compliance; and
  - Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls;

- Reviews and updates the current:
  - Audit and accountability policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Audit and accountability procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop document, review/update agency-wide audit and accountability control policy and procedures, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific audit procedures are developed, reviewed/updated, and maintained for all system components in accordance with NRC requirements.
- Ensure that system-specific audit procedures facilitate the implementation of the audit and accountability policy.

4.1.3.2 AU-2 Audit Events

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Determines that the information system is capable of auditing the NRC-defined required events in accordance with CSO-STD-0020 and other NRC requirements;
- Coordinates the security audit function with other NRC entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
- Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
- Determines the NRC-defined audited events to be audited within the information system, along with the frequency of (or situation requiring) auditing for each identified event in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Identify the auditable events that must be captured in NRC systems.

- Define the subset of auditable events that NRC systems must be capable of auditing.
- Define the frequency of auditing for each identified event in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Identify auditable events that should be captured in the system in accordance with CSO-STD-0020 and other NRC requirements.
- Ensure that audit functions are coordinated with other NRC entities to enhance mutual support and to help guide the selection of auditable events.
- Provide required rationale for auditable event selection for the system.
- Ensure system-specific auditable events are captured in accordance with NRC requirements.
- Ensure systems are capable of auditing the subset of auditable events that NRC systems must be capable of auditing.

4.1.3.2.1 AU-2[3] Reviews and Updates

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The organization reviews and updates the audited events in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Ensure the list of NRC-defined auditable events is reviewed and updated in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that system-specific auditable events are reviewed and updated in accordance with CSO-STD-0020 and other NRC requirements.

4.1.4 Security Assessment and Authorization

Table 4.1-4 summarizes the common and hybrid security control responsibilities for the CA family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-4: CA Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
CA-1	Security Assessment and Authorization Policy and Procedures	CSO, System Owners	Hybrid
CA-2	Security Assessments	CSO, System Owners	Hybrid
CA-2[1]	Independent Assessors	CSO, System Owners	Hybrid
CA-2[2]	Specialized Assessments	CSO	Common
CA-3	System Interconnections	CSO, System Owners	Hybrid
CA-3[5]	Restrictions on External System Connections	CSO, OIS, System Owners	Hybrid
CA-5	Plan of Action and Milestones	System Owners	System Specific
CA-6	Security Authorization	OEDO, CSO, System Owners	Hybrid
CA-7	Continuous Monitoring	CSO, System Owners	Hybrid
CA-7[1]	Independent Assessment	OEDO, CSO, System Owners	Hybrid
CA-8	Penetration Testing	CSO	Common
CA-9	Internal System Connections	System Owners	System Specific

4.1.4.1 CA-1 Security Assessment and Authorization Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls;
- Reviews and updates the current:
  - Security assessment and authorization policy in accordance with CSO-STD-0020 and other NRC requirements; and

- Security assessment and authorization procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide security assessment and authorization control policy, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific security assessment and authorization procedures are developed, reviewed/updated, and maintained for the system in accordance with CSO-STD-0020 and other NRC requirements.
- Ensure that system-specific security assessment and authorization procedures facilitate the implementation of the security assessment and authorization policy.

4.1.4.2 CA-2 Security Assessments

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops a security assessment plan that describes the scope of the assessment including:
  - Security controls and control enhancements under assessment;
  - Assessment procedures to be used to determine security control effectiveness; and
  - Assessment environment, assessment team, assessment roles and responsibilities;
- Assesses the security controls in the systems and its environment of operation in accordance with CSO-STD-0020 and other NRC requirements 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;
- Produces a security assessment report that documents the results of the assessment; and
- Provides the results of the security control assessment to the NRC-defined individuals or roles in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Provide policy, assessment plan and report templates, and define the minimum frequency for assessing security controls.
- Provide requirements for conducting security control testing and define the core controls that must be tested.

System owners must:

- Ensure system's security controls are assessed in accordance with CSO-STD-0020 and other NRC requirements.
- Initiate assessment tasks with the independent assessment team and ensure that assessment plans and assessment reports are developed and documented in accordance with NRC requirements and provided to the CSO.

4.1.4.2.1 CA-2[1] Independent Assessors

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC employs assessors or assessment teams in accordance with CSO-STD-0020 and other NRC requirements to conduct security control assessments.

Provider Responsibilities:

CSO must:

- Provide a contract vehicle that includes an independent assessment team.

System owners must:

- Budget and schedule security assessments (e.g., periodic authorization, on-going authorization, change authorization) with an independent assessment team in accordance with NRC requirements.

4.1.4.2.2 CA-2[2] Specialized Assessments

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC includes as part of security control assessments, an NRC-defined frequency, announced and/or unannounced, one or more of the following: in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, management initiated review of a control, performance/load testing; or other forms of NRC-defined security assessment.

Provider Responsibilities:

CSO must:

- Provide coordination and oversight for specialized assessments.

4.1.4.3 CA-3 System Interconnections

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Authorizes connections from one information system to another information system through the use of Interconnection Security Agreements (ISAs);
- Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
- Reviews and updates ISAs in accordance with CSO-STD-0020 and other NRC requirements.

NRC Supplemental Information:

NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," provides the following definition:

"System Interconnection: The direct connection of two or more IT systems for the purpose of sharing data and other information resources."

Provider Responsibilities:

CSO must:

- Provide policy for system interconnections within NRC and with external systems and provide the Memorandum of Understanding (MOU) and ISA templates.

System owners must:

- Document the interface characteristics, security requirements, and the nature of the information communicated, for each system connection.
- Review and update, if necessary, the ISA in accordance with CSO-STD-0020 and other NRC requirements.
- Ensure that the agreed upon set of security controls that govern these connections are maintained and operating as intended.
- Ensure that the CIO approves/signs all connections and agreements between an NRC system and another federal agency system or a system owned by another party as

defined in MD 12.5, “NRC Cyber Security Program,” Section III, Part E, under “Organizational Responsibilities and Delegations of Authority.”

4.1.4.3.1 CA-3[5] Restrictions on External System Connections

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC employs a deny-all, permit-by-exception policy for allowing NRC information systems to connect to external information systems.

Provider Responsibilities:

CSO must:

- Provide interconnection requirements for external system connections.

OIS must:

- Provide boundary devices at the perimeter to enforce a deny-all, permit-by-exception policy for those systems on the NRC LAN/Wide Area Network (WAN).

System owners must:

- Ensure that boundary devices employ a deny-all, permit-by-exception policy for allowing NRC information systems to connect to external information systems in accordance with NRC requirements.

4.1.4.4 CA-6 Security Authorization

This is a ***hybrid*** security control with responsibilities for the **OEDO**, **CSO**, and **system owners**.

Control Description:

The NRC:

- Assigns a senior-level executive or manager as the authorizing official for the information system;
- Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
- Updates the security authorization in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

OEDO must:

- Appoint the DAA and identify the DAA's responsibilities to facilitate NRC compliance with the requirements imposed by FISMA and related policies, procedures, standards, and guidelines.

CSO must:

- Provide security authorization policy and guidance, and define the frequency and conditions for updating security authorizations.
- Provide recommendations to the DAAs for approving or denying system authorizations.

System owners must:

- Ensure the system has an authority to operate (ATO) from the DAA before being placed into the operational environment.
- Update the security authorization in accordance with CSO-STD-0020 and other NRC requirements.

4.1.4.5 CA-7 Continuous Monitoring

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

- Establishment of NRC-defined metrics to be monitored in accordance with CSO-STD-0020, CSO-PROS-1323, "Information Security Continuous Monitoring Process," and other NRC requirements;
- Establishment of NRC-defined frequencies for monitoring and for assessments supporting such monitoring in accordance with CSO-STD-0020, CSO-PROS-1323, and other NRC requirements;
- Ongoing security control assessments in accordance with CSO-PROS-1323;
- Ongoing security status monitoring of NRC-defined metrics in accordance with CSO-STD-0020, CSO-PROS-1323, and other NRC requirements;
- Correlation and analysis of security-related information generated by assessments and monitoring;
- Response actions to address results of the analysis of security-related information; and
- Reporting the security status of NRC and the information system in accordance with CSO-STD-0020, CSO-PROS-1323, and other NRC requirements.

Provider Responsibilities:

CSO must:

- Provide continuous monitoring policy and requirements, and establish the NRC-defined metrics to support the NRC continuous monitoring program along with their respective frequencies.

System owners must:

- Ensure that the security state of the system adheres to NRC continuous monitoring requirements in accordance with CSO-STD-0020, CSO-PROS-1323, and other NRC requirements.
- Conduct ongoing security control assessments in accordance with the NRC continuous monitoring strategy.
- Correlate and analyze security-related information generated by assessments and monitoring.
- Address results of the analysis of security-related information and report the security status of the system in accordance with CSO-STD-0020, CSO-PROS-1323, and other NRC requirements.

4.1.4.5.1 CA-7[1] Independent Assessment

This is a ***hybrid*** security control with responsibilities for the **OEDO**, **CSO**, and **system owners**.

Control Description:

The NRC employs assessors or assessment teams in accordance with CSO-STD-0020, CSO-PROS-1323, and other NRC requirements to monitor the security controls in the information system on an ongoing basis.

Provider Responsibilities:

OEDO must:

- Approve independent assessors.

CSO must:

- Define the independence level needed for monitoring security controls on an ongoing basis.

System owners must:

- Budget and schedule independent assessment teams in accordance with CSO-STD-0020, CSO-PROS-1323, and other NRC requirements to monitor security controls in the information system on an ongoing basis.

4.1.4.6 CA-8 Penetration Testing

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC conducts penetration testing in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Conduct penetration testing on NRC-defined systems or system components in accordance with CSO-STD-0020 and other NRC requirements.

4.1.5 Configuration Management

Table 4.1-5 summarizes the common and hybrid security control responsibilities for the CM family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-5: CM Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
CM-1	Configuration Management Policy and Procedures	CSO, OIS, System Owners	Hybrid
CM-2	Baseline Configuration	System Owners	System Specific
CM-2[1]	Review and Updates	System Owners	System Specific
CM-2[2]	Automation Support for Accuracy	System Owners	System Specific
CM-2[3]	Retention of Precious Configurations	System Owners	System Specific
CM-2[7]	Configure Systems, Components, or Devices for High Risk Areas	System Owners	System Specific
CM-3	Configuration Change Control	System Owners	System Specific
CM-3[1]	Automated Document / Notification / Prohibition of Changes	System Owners	System Specific
CM-3[2]	Test / Validate / Document Changes	System Owners	System Specific
CM-4	Security Impact Analysis	CSO, System Owners	Hybrid
CM-4[1]	Separate Test Environments	System Owners	System Specific
CM-5	Access Restrictions for Change	System Owners	System Specific
CM-5[1]	Automated Access Enforcement / Auditing	System Owners	System Specific
CM-5[2]	Review System Changes	System Owners	System Specific

Control ID	Control Title	Provider(s)	Control Type
CM-5[3]	Signed Components	System Owners	System Specific
CM-6	Configuration Settings	CSO, System Owners	Hybrid
CM-6[1]	Automated Central Management / Application / Verification	System Owners	System Specific
CM-6[2]	Respond to Unauthorized Changes	System Owners	System Specific
CM-7	Least Functionality	System Owners	System Specific
CM-7[1]	Periodic Review	System Owners	System Specific
CM-7[2]	Prevent Program Execution	System Owners	System Specific
CM-7[4]	Unauthorized Software / Blacklisting	System Owners	System Specific
CM-7[5]	Authorized Software / Whitelisting	System Owners	System Specific
CM-8	Information System Component Inventory	System Owners	System Specific
CM-8 [1]	Updates During Installations / Removals	System Owners	System Specific
CM-8[2]	Automated Maintenance	System Owners	System Specific
CM-8[3]	Automated Unauthorized Component Detection	System Owners	System Specific
CM-8[4]	Accountability Information	System Owners	System Specific
CM-8[5]	No Duplicate Accounting of Components	System Owners	System Specific
CM-9	Configuration Management Plan	System Owners	System Specific
CM-10	Software Usage Restrictions	System Owners	System Specific
CM-11	User-Installed Software	CSO, System Owners	Hybrid

4.1.5.1 CM-1 Configuration Management Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A configuration management policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls;

- Reviews and updates the current:
  - Configuration management policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Configuration management procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide configuration management control policy, define the frequency for reviews and updates, and distribute to NRC users.

OIS must:

- Provide policy and guidance for centralizing, managing, and approving IT configuration changes across the NRC.

System owners must:

- Ensure that system-specific configuration management procedures are developed, reviewed/updated, and maintained for the systems in accordance with NRC requirements.
- Ensure that system-specific configuration management procedures facilitate the implementation of the configuration management policy.

4.1.5.2 CM-4 Security Impact Analysis

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC analyzes changes to the information system to determine potential security impacts prior to change implementation.

Provider Responsibilities:

CSO must:

- Provide policy, requirements and templates for the NRC system change process.
- Analyze system change deliverables to identify potential cybersecurity issues as early in the process as possible, and make a cybersecurity risk-based recommendation to the DAA regarding authorization of change deployment for all non-minor changes.

System owners must:

- Conduct initial assessments to evaluate security impacts prior to purchase.
- Ensure system changes are conducted in accordance with CSO-PROS-1321, “System Cybersecurity Coordination Process for New Systems and System Changes.”
- Analyze changes to the system to determine potential security impacts prior to change implementation

4.1.5.3 CM-6 Configuration Settings

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Establishes and documents configuration settings for information technology products employed within the information system in accordance with NRC requirements that reflect the most restrictive mode consistent with operational requirements;
- Implements the configuration settings;
- Identifies, documents, and approves any deviations from established configuration settings for configurable information system components in accordance with CSO-PROS-1324, “NRC Deviation Request Process;” and
- Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Provider Responsibilities:

CSO must:

- Establish and document mandatory configuration standards for NRC IT resources that reflect the minimum requirements. These minimum requirements reflect the most restrictive mode that is consistent with operational requirements. CSO standards and external standards located on the CSO web page are used to establish the NRC’s CM baseline for all NRC IT resources.

System owners must:

- Ensure that configuration settings are established, documented, and monitored and controlled in accordance with NRC requirements that reflect the most restrictive mode consistent with operational requirements.
- Monitor and control changes to the configuration settings in accordance with NRC requirements.
- Ensure that deviations from mandatory configuration settings are identified, documented and submitted for approval in accordance with CSO-PROS-1324.

4.1.5.4 CM-11 User-Installed Software

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Establishes policy governing the installation of software by users in accordance with the NRC MDs and the "Agency-wide Rules of Behavior;"
- Enforces NRC software installation policies in accordance with CSO-STD-0020 and other NRC requirements; and
- Monitors policy compliance using NRC automated security applications, in accordance with CSO-PROS-1323.

Provider Responsibilities:

CSO must:

- Establish and document policy and requirements regarding the installation of software by NRC users.

System owners must:

- Ensure the system complies with NRC policy governing user-installed software in accordance with the NRC MDs, CSO-PROS-1323, and the "Agency-wide Rules of Behavior."
- Ensure that the installation of unauthorized software programs is monitored in accordance with CSO-STD-0020 and other NRC requirements.

4.1.6 Contingency Planning

Table 4.1-6 summarizes the common and hybrid security control responsibilities for the CP family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-6: CP Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
CP-1	Contingency Planning Policy and Procedures	CSO, System Owners	Hybrid
CP-2	Contingency Plan	System Owners	System Specific
CP-2[1]	Coordinate with Related Plan	System Owners	System Specific
CP-2[2]	Capacity Planning	System Owners	System Specific
CP-2[3]	Resume Essential Missions / Business Functions	System Owners	System Specific
CP-2[4]	Resume All Missions / Business Functions	System Owners	System Specific

Control ID	Control Title	Provider(s)	Control Type
CP-2[5]	Continue Essential Missions / Business Functions	System Owners	System Specific
CP-2[8]	Identify Critical Assets	System Owners	System Specific
CP-3	Contingency Training	System Owners	System Specific
CP-3[1]	Simulated Events	System Owners	System Specific
CP-4	Contingency Plan Testing	System Owners	System Specific
CP-4[1]	Coordinate with Related Plans	System Owners	System Specific
CP-4[2]	Alternate Processing Site	System Owners	System Specific
CP-6	Alternate Storage Site	System Owners	System Specific
CP-6[1]	Separation from Primary Site	System Owners	System Specific
CP-6[2]	Recovery Time / Point Objectives	System Owners	System Specific
CP-6[3]	Accessibility	System Owners	System Specific
CP-7	Alternate Processing Site	System Owners	System Specific
CP-7[1]	Separation from Primary Site	System Owners	System Specific
CP-7[2]	Accessibility	System Owners	System Specific
CP-7[3]	Priority of Service	System Owners	System Specific
CP-7[4]	Preparation for Use	System Owners	System Specific
CP-8	Telecommunications Services	CSO, OIS, Regional Administrators, System Owners	Hybrid
CP-8[1]	Priority of Service Provisions	OIS, Regional Administrators, System Owners	Hybrid
CP-8[2]	Single Points of Failure	OIS, Regional Administrators, System Owners	Hybrid
CP-8[3]	Separation of Primary / Alternate Providers	OIS, Regional Administrators, System Owners	Hybrid
CP-8[4]	Provider Contingency Plan	OIS, Regional Administrators, System Owners	Hybrid
CP-9	Information System Backup	System Owners	System Specific
CP-9[1]	Testing for Reliability/Integrity	System Owners	System Specific
CP-9[2]	Test Restoration Using Sampling	System Owners	System Specific
CP-9[3]	Separate Storage for Critical Information	System Owners	System Specific
CP-9[5]	Transfer ro Alternate Storage site	System Owners	System Specific
CP-10	Information System Recovery and Reconstitution	System Owners	System Specific
CP-10[2]	Transaction Recovery	System Owners	System Specific
CP-10[4]	Protections From Unauthorized Modification	System Owners	System Specific

4.1.6.1 CP-1 Contingency Planning Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A contingency planning policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls;
- Reviews and updates the current:
  - Contingency planning policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Contingency planning procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update NRC contingency planning control policy, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific contingency planning procedures are developed, reviewed/updated and maintained for the systems in accordance with NRC requirements.
- Ensure that system-specific contingency planning procedures facilitate the implementation of the contingency planning policy.

4.1.6.2 CP-8 Telecommunications Services

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, **Regional Administrators**, and **system owners**.

Control Description:

The NRC establishes alternate telecommunication services including necessary agreements to permit the resumption of information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define the timeframes for the system owner to establish alternate telecommunications services when the primary telecommunications capabilities are unavailable.

OIS must:

- Provide alternate telecommunications services, including necessary agreements to permit the resumption of information system operations for:
  - Essential mission and business functions for NRC systems located at NRC facilities; and
  - Agency-wide essential mission and business functions (e.g., Internet access) for NRC systems located at all NRC facilities.

Regional Administrators must:

- Ensure the systems hosted in the regions establish alternate telecommunications services for essential mission and business functions, which the respective regional office is responsible for (e.g., telephone services) in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Develop and maintain necessary agreements with OIS for alternate telecommunications services in accordance with CSO-STD-0020 and other NRC requirements.
- Ensure the systems not hosted at NRC facilities establish alternate telecommunications services in accordance with CSO-STD-0020 and other NRC requirements.

4.1.6.2.1 CP-8[1] Priority of Service Provisions

This is a ***hybrid*** security control with responsibilities for **OIS**, **Regional Administrators**, and **system owners**.

Control Description:

The NRC:

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

Provider Responsibilities:

OIS must:

- Provide primary and alternate telecommunications service agreements (e.g., Internet access) that contain priority-of-service provisions in accordance with organizational availability requirements for NRC systems hosted at NRC facilities.

Regional Administrators must:

- Ensure the systems hosted in the regions establish primary and alternate telecommunications service agreements (e.g., telephone services) that contain priority-of-service provisions.

System owners must:

- Develop and maintain necessary agreements with OIS for primary and alternate telecommunications service agreements that contain priority-of-service provisions for systems hosted at NRC facilities.
- Ensure that NRC systems hosted in non-NRC facilities establish primary and alternate telecommunications service agreements that contain priority-of-service provisions.

4.1.6.2.2 CP-8[2] Single Points of Failure

This is a ***hybrid*** security control with responsibilities for **OIS**, **Regional Administrators**, and **system owners**.

Control Description:

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

Provider Responsibilities:

OIS must:

- Provide alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services (e.g., Internet access) for NRC systems hosted at NRC facilities.

Regional Administrators must:

- Ensure the systems hosted in the regions establish alternate telecommunications services (e.g., telephone services) to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

System owners must:

- Develop and maintain necessary agreements with OIS for services to reduce the likelihood of sharing a single point of failure with primary telecommunications services for systems hosted at NRC facilities.
- Ensure that NRC systems hosted in non-NRC facilities establish services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

4.1.6.2.3 CP-8[3] Separation of Primary / Alternate Providers

This is a ***hybrid*** security control with responsibilities for **OIS**, **Regional Administrators**, and **system owners**.

Control Description:

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

Provider Responsibilities:

OIS must:

- Provide alternate telecommunications services (e.g., Internet access) from providers that are separated from primary service providers to reduce susceptibility to the same threats for NRC systems hosted at NRC facilities.

Regional Administrators must:

- Ensure the systems hosted in the regions establish alternate telecommunications services (e.g., telephone services) from providers that are separated from primary service providers to reduce susceptibility to the same threats.

System owners must:

- Develop and maintain necessary agreements with OIS for alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats for systems hosted at NRC facilities.
- Ensure the NRC systems hosted in non-NRC facilities establish alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

4.1.6.2.4 CP-8[4] Provider Contingency Plan

This is a ***hybrid*** security control with responsibilities for **OIS**, **Regional Administrators**, and **system owners**.

Control Description:

The NRC:

- Requires primary and alternate telecommunications service providers to have contingency plans; and
- Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements.

Provider Responsibilities:

OIS must:

- Require primary and alternate telecommunications service providers (e.g., Internet access) to have contingency plans that meet organizational contingency requirements for NRC systems hosted at NRC facilities.

Regional Administrators must:

- Ensure the systems hosted in the regions require primary and alternate telecommunications service providers (e.g., telephone services) to have contingency plans that meet organizational contingency requirements.

System owners must:

- Develop and maintain necessary agreements with OIS for alternate telecommunications services (e.g., Internet access) that requires providers to have contingency plans that meet organizational contingency requirements for NRC systems hosted at NRC facilities.
- Ensure that NRC systems hosted in non-NRC facilities require primary and alternate telecommunications service providers to have contingency plans that meet organizational contingency requirements.

4.1.7 Identification and Authentication

Table 4.1-7 summarizes the common and hybrid security control responsibilities for the IA family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-7: IA Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
IA-1	Identification and Authentication Policy and Procedures	CSO, System Owners	Hybrid
IA-2	Identification and Authentication (Organizational Users)	CSO, OIS, System Owners	Hybrid
IA-2[1]	Network Access to Privileged Accounts	System Owners	System Specific
IA-2[2]	Network Access to Non-Privileged Accounts	System Owners	System Specific
IA-2[3]	Local Access to Privileged Accounts	System Owners	System Specific
IA-2[4]	Local Access to Non-Privileged Accounts	System Owners	System Specific
IA-2[8]	Network Access to Privileged Accounts – Replay Resistant	System Owners	System Specific
IA-2[9]	Network Access to Non-Privileged Accounts – Replay Resistant	System Owners	System Specific
IA-2[11]	Remote Access – Separate Device	System Owners	System Specific
IA-2[12]	Acceptance of PIV Credentials	System Owners	System Specific
IA-3	Device Identification and Authentication	System Owners	System Specific
IA-4	Identifier Management	CSO, OIS, System Owners	Hybrid
IA-5	Authenticator Management	CSO, OIS, System Owners	Hybrid
IA-5[1]	Password-Based Authentication	CSO, OIS, System Owners	Hybrid
IA-5[2]	PKI-Based Authentication	OIS, System Owners	Hybrid
IA-5[3]	In-Person or Trusted Third-Party Registration	Office of Administration (ADM), System Owners	Hybrid
IA-5[11]	Hardware Token-Based Authentication	OIS, System Owners	Hybrid
IA-6	Authenticator Feedback	System Owners	System Specific
IA-7	Cryptographic Module Authentication	CSO, OIS, System Owners	Hybrid
IA-8	Identification and Authentication (Non-Organizational Users)	System Owners	System Specific
IA-8[1]	Acceptance of PIV Credentials From Other	System Owners	System Specific

Control ID	Control Title	Provider(s)	Control Type
	Agencies		
IA-8[2]	Acceptance of Third-Party Credentials	System Owners	System Specific
IA-8[3]	Use of FICAM-Approved Products	System Owners	System Specific
IA-8[4]	Use of FICAM-Issued Profiles	System Owners	System Specific

4.1.7.1 IA-1 Identification and Authentication Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - An identification and authentication policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls;
- Reviews and updates the current:
  - Identification and authentication policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Identification and authentication procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide identification and authentication control policy, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific identification and authentication procedures are developed, reviewed/updated, and maintained for the systems in accordance with NRC requirements.
- Ensure that system-specific identification and authentication procedures facilitate the implementation of identification and authentication policy.

4.1.7.2 IA-2 Identification and Authentication (Organizational Users)

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Provider Responsibilities:

CSO must:

- Provide policy and requirements for identification and authentication for NRC users (or processes acting on behalf of organizational users).

OIS must**:**

- Uniquely identify and authenticate NRC users for NRC managed networks Windows-based systems integrated with AD userids and passwords. Systems that require separate and distinct login credentials **cannot inherit this control** and must implement system-specific identification and authentication mechanisms in accordance with NRC requirements.
- Uniquely identify and authenticate processes acting on behalf of NRC users for NRC managed networks Windows-based systems integrated with AD userids and passwords. Systems that require separate and distinct login credentials **cannot inherit this control** and must implement system-specific identification and authentication mechanisms in accordance with NRC requirements.

System owners must:

- Ensure that the system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) in accordance with NRC requirements.

4.1.7.3 IA-4 Identifier Management

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC manages information system identifiers by:

- Receiving authorization from the system owners to assign an individual, group, role, or device identifier;
- Selecting an identifier that identifies an individual, group, role, or device;
- Assigning the identifier to the intended individual, group, role, or device;

- Preventing reuse of identifiers in accordance with CSO-STD-0020 and other NRC requirements; and
- Disabling the identifier in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Provide policy and requirements for managing system identifiers.

OIS must**:**

- Manage system identifiers for NRC managed networks Windows-based systems integrated with AD. Systems that require separate and distinct login credentials **cannot inherit this control** and must manage system identifiers in accordance with NRC requirements.

System owners must:

- Ensure the system manages system identifiers in accordance with CSO-STD-0020.

4.1.7.4 IA-5 Authenticator Management

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC manages information system authenticators by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- Establishing initial authenticator content for authenticators defined by the organization;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators prior to information system installation;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- Changing/refreshing authenticators in accordance with CSO-STD-0020 and other NRC requirements.
- Protecting authenticator content from unauthorized disclosure and modification;

- Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- Changing authenticators for group/role accounts when membership to those accounts changes.

Provider Responsibilities:

CSO must:

- Provide policy and requirements for managing system authenticators.

OIS must**:**

- Manage system authenticators for NRC managed networks Windows-based systems integrated with AD. Systems that require separate and distinct login credentials **cannot inherit this control** and must implement **system-specific** authentication mechanisms in accordance with NRC requirements.

System owners must:

- Verify, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
- Establish initial authenticator content for authenticators.
- Ensure that authenticators have sufficient strength of mechanism for their intended use.
- Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
- Change default content of authenticators prior to information system installation.
- Change/refresh authenticators in accordance with CSO-STD-0020 and other NRC requirements.
- Protect authenticator content from unauthorized disclosure and modifications.
- Change authenticators for group/role accounts when membership to those accounts changes.

4.1.7.4.1 IA-5[1] Password-Based Authentication

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Enforces minimum password complexity in accordance with CSO-STD-0001, “NRC Strong Password Standard;”

- Enforces the number of changed characters when new passwords are created in accordance with CSO-STD-0001;
- Stores and transmits only cryptographically-protected passwords;
- Enforces password minimum and maximum lifetime restriction requirements in accordance with CSO-STD-0001;
- Prohibits password reuse in accordance with CSO-STD-0001; and
- Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Provider Responsibilities:

CSO must:

- Define the standard for the creation of passwords to protect NRC sensitive information and information systems.

OIS must**:**

- Manage the system authenticators for NRC managed networks Windows-based systems integrated with AD in accordance with CSO-STD-0001. Systems that require separate and distinct login credentials **cannot inherit this control** and must implement **system-specific** authentication mechanisms in accordance with NRC requirements.

System owners must:

- Ensure that the minimum password complexity is enforced in accordance with CSO-STD-0001.
- Ensure that the number of changed characters when new passwords are created in accordance with CSO-STD-0001.
- Ensure that the system stores and transmits only cryptographically-protected passwords.
- Ensure that the password minimum and maximum lifetime restriction requirements is enforced in accordance with CSO-STD-0001.
- Ensure that password reuse requirements are in accordance with CSO-STD-0001.
- Allow the use of a temporary password for system logons with an immediate change to a permanent password.

4.1.7.4.2 IA-5[2] PKI-Based Authentication

This is a hybrid security control with responsibilities for the **OIS** and **system owners**.

Control Description:

The NRC for Public Key Interface (PKI)-based authentication:

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
- Enforces authorized access to the corresponding private key;
- Maps the authenticated identity to the account of the individual or group; and
- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Provider Responsibilities:

OIS must**:**

- Manage PKI-based authentication for NRC managed networks Windows-based systems integrated with AD in accordance with CSO-STD-0001 and CSO-STD-2009.

System owners must:

- Ensure the system manages PKI-based authentication in accordance with CSO-STD-0001 and CSO-STD-2009.

4.1.7.4.3 IA-5[3] In-Person or Trusted Third-Party Registration

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**.

Control Description:

The NRC 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. The registration process is the initial registration process and does not apply to renewals as long as the identity-proofing instance used as the basis for issuing the credential has not expired. If the identity-proofing instance has expired, the registration process must be used, including in person identity verification.

Provider Responsibilities:

ADM must**:**

- Provide and manage the in-person registration process before a designated registration authority for issuance of the Personal Identity Verification (PIV) card for NRC staff and contractors.

System owners must:

- Ensure that the authenticator issuance for access to the system is performed in accordance with the current, published version of NIST SP 800-63, “Electronic Authentication Guideline” and CSO-STD-2009.
- Ensure that digital certificate issuance for access to unclassified systems is performed in accordance with the current, published version of the Federal Bridge Certification Authority (FBCA) X.509 Certificate Policy.

4.1.7.4.4 IA-5[11] Hardware Token-Based Authentication

This is a ***hybrid*** security control with responsibilities for the **OIS** and **system owners**.

Control Description:

The NRC employs for hardware token-based authentication, mechanisms that satisfy token quality requirements defined in Federal Information Processing Standards (FIPS) 201-2, “Personal Identity Verification (PIV) of Federal Employees and Contractors.”

Provider Responsibilities:

OIS must**:**

- Provide the mechanisms that satisfy token quality requirements defined in FIPS 201-2.

System owners must:

- Ensure that hardware token-based authentication for the system satisfies the token quality requirements defined in FIPS 201-2.

4.1.7.5 IA-7 Cryptographic Module Authentication

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC 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.

Provider Responsibilities:

CSO must:

- Provide policy and requirements for cryptographic module authentication.

OIS must**:**

- Implement mechanisms for authentication to a cryptographic module for NRC managed networks Windows-based systems integrated with AD. Systems that require separate and distinct login credentials **cannot inherit this control** and must implement mechanisms for authentication to a cryptographic module in accordance with NRC requirements.

System owners must:

- Ensure the system implements mechanisms for authentication to a cryptographic module in accordance with NRC requirements.

4.1.8 Incident Response

Table 4.1-8 summarizes the common and hybrid security control responsibilities for the IR family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-8: IR Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
IR-1	Incident Response Policy and Procedures	CSO, System Owners	Hybrid
IR-2	Incident Response Training	CSO, System Owners	Hybrid
IR-2[1]	Simulated Events	CSO, System Owners	Hybrid
IR-2[2]	Automated Training Environments	CSO, System Owners	Hybrid
IR-3	Incident Response Testing	CSO, System Owners	Hybrid
IR-3[2]	Coordination with Related Plans	System Owners	System Specific
IR-4	Incident Handling	CSO, System Owners	Hybrid
IR-4[1]	Automated Incident Handling Processes	CSO, System Owners	Hybrid
IR-4[4]	Information Correlation	CSO, System Owners	Hybrid
IR-5	Incident Monitoring	CSO, System Owners	Hybrid
IR-5[1]	Automated Tracking / Data Collection / Analysis	CSO, System Owners	Hybrid
IR-6	Incident Reporting	CSO, System Owners	Hybrid
IR-6[1]	Automated Reporting	CSO	Common
IR-7	Incident Response Assistance	CSO, OIS	Common
IR-7[1]	Automation Support for Availability of Information / Support	CSO	Common
IR-8	Incident Response Plan	CSO, System Owners	Hybrid

4.1.8.1 IR-1 Incident Response Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - An incident response policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the incident response policy and associated incident response controls;
- Reviews and updates the current:
  - Incident response policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Incident response procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide incident response control policy and procedures, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific incident response procedures are developed, reviewed/updated, and maintained for the systems in accordance with NRC requirements.
- Ensure that system-specific incident response procedures facilitate the implementation of incident response policy.

4.1.8.2 IR-2 Incident Response Training

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC provides incident response training to information system users consistent with assigned roles and responsibilities:

- Within the NRC-defined time period of assuming an incident response role or responsibility in accordance with CSO-STD-0020 and other NRC requirements;
- When required by information system changes; and

- Within the NRC-defined frequency thereafter in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Provide incident response training to the agency-wide incident response team that includes incident response scenarios and incident handling. The Cyber, Situational, Awareness, Analysis, and Response (CSAAR) Senior Information Technology Security Officer (SITSO) must provide specialized training to the Cybersecurity Incident Response Team (CSIRT) members within 30 days of assuming an IR role or responsibility and refresher training at least annually thereafter.

System owners must:

- Ensure that system-specific incident response training is provided for those personnel with assigned responsibilities for incident response.

4.1.8.2.1 IR-2[1] Simulated Events

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Provider Responsibilities:

CSO must:

- Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations. Specialized training includes using simulated events, to facilitate an effective response by personnel during crisis situations, and other automated mechanisms to provide a more robust and realistic training environment, as appropriate.

System owners must:

- Ensure that simulated events are incorporated into system-specific incident response training to facilitate effective response during a crisis situation.

4.1.8.2.2 IR-2[2] Automated Training Environments

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC employs automated mechanisms to provide a more thorough and realistic incident response training environment.

Provider Responsibilities:

CSO must:

- Provide specialized training to the CSIRT members using automated mechanisms to provide a more thorough and realistic incident response training environment.

System owners must:

- Ensure that automated mechanisms are employed in system-specific training to provide a more thorough and realistic training environment for those personnel with incident response responsibilities.

4.1.8.3 IR-3 Incident Response Testing

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC tests the incident response capability for the information system in accordance with CSO-STD-0020 and other NRC requirements to determine the incident response effectiveness and documents the results.

Provider Responsibilities:

CSO must:

- Define the frequency and types of tests for incident response testing in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that incident response testing is conducted for the system in accordance with CSO-STD-0020 and other NRC requirements.

4.1.8.4 IR-4 Incident Handling

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Provider Responsibilities:

CSO (CSIRT) must:

- Implement an incident handling capability for NRC security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
- Coordinate incident handling activities with contingency planning activities.
- Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

System owners must:

- Implement system-specific incident handling procedures to address all phases (e.g., preparation, detection and analysis, containment, eradication and recovery) of an incident.
- Coordinate incident handling activities with contingency planning activities.
- Notify and coordinate all incident-handling activities with CSO CSIRT.

4.1.8.4.1 IR-4[1] Automated Incident Handling Processes

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC employs automated mechanisms to support the incident handling process.

Provider Responsibilities:

CSO (CSIRT) must:

- Provide automated incident response mechanisms (e.g., NRC email, posting of network announcements on NRC internal web page, yellow announcements) to support the incident handling process.

System owners must:

- Ensure that automated mechanisms (e.g., email, incident management software) are implemented to support the system-specific incident handling process.

4.1.8.4.2 IR-4[4] Information Correlation

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Provider Responsibilities:

CSO (CSIRT) must:

- Correlate incident information and individual incident responses to achieve an NRC perspective on incident awareness and response.

System owners must:

- Ensure that system-specific incident information is correlated and reported to CSO to gain perspective on incident awareness and response.

4.1.8.5 IR-5 Incident Monitoring

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC tracks and documents information system security incidents.

Provider Responsibilities:

CSO (CSIRT) must:

- Track and document NRC information security incidents.
- Report NRC information security incidents to appropriate authorities.

System owners must:

- Ensure that all security incidents are documented and reported to CSO CSIRT in accordance with NRC requirements.

4.1.8.5.1 IR-5[1] Automated Tracking / Data Collection / Analysis

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Provider Responsibilities:

CSO (CSIRT) must:

- Employ automated mechanisms (e.g., incident management software) to assist in the tracking of security incidents. The use of these tools enables the CSIRT to collect, report, track, and analyze computer security related incidents.

System owners must:

- Ensure that automated mechanisms (e.g., incident management software) are used to assist in the tracking of security incidents and capturing incident information.

4.1.8.6 IR-6 Incident Reporting

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Requires personnel to report suspected security incidents to the NRC incident response capability in accordance with CSO-STD-0020 and other NRC requirements; and
- Reports security incident information to NRC-defined authorities.

Provider Responsibilities:

CSO (CSIRT) must:

- Require NRC personnel to report suspected security incidents to the NRC incident response capability in accordance with CSO-STD-0020 and other NRC requirements.
- Report security incident information to NRC-defined authorities in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Report all suspected security incidents to CSO in accordance with CSO-STD-0020, CSIRT Incident Response Standard Operating Procedures, and other NRC requirements.

4.1.8.6.1 IR-6[1] Automated Reporting

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC employs automated mechanisms to assist in the reporting of security incidents.

Provider Responsibilities:

CSO (CSIRT) must:

- Employ a secure automated mechanism (e.g., incident management software) for reporting computer security related incidents in accordance with United States Computer Emergency Readiness Team (US-CERT) guidelines.

4.1.8.7 IR-7 Incident Response Assistance

This is a **common** security control with responsibilities for the **CSO** and **OIS**.

Control Description:

The NRC provides an incident response support resource, integral to the agency incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Provider Responsibilities:

CSO (CSIRT) must:

- Provide an incident response support resource, integral to the agency incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

OIS must:

- Provide, manage and maintain the NRC Customer Support Center (CSC) as an additional incident support resource for NRC users.

4.1.8.7.1 IR-7[1] Automation Support for Availability of Information / Support

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC employs automated mechanisms to increase the availability of incident response-related information and support.

Provider Responsibilities:

CSO (CSIRT) must:

- Employ automated mechanisms (e.g., NRC email, posting of network announcements on NRC internal web page, yellow announcements) to increase the availability of incident response-related information and support

4.1.8.8 IR-8 Incident Response Plan

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC develops an incident response plan that:

- Provides the organization with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall organization;
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the organization;
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved initially by NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

The **CSO** incident response plan must:

- Provide NRC with a roadmap for implementing its incident response capability.
- Describe the structure and organization of the incident response capability.
- Provide a high-level approach for how the incident response capability fits into the overall organization.

- Meet the unique requirements for NRC, which relate to mission, size, structure, and functions.
- Define reportable incidents.
- Provide metrics for measuring the incident response capability within the NRC.
- Define the resources and management support needed to effectively maintain and mature an incident response capability; and
- Be reviewed and approved initially by NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements

System owners must:

- Describe the structure and organization of the system's incident response capability.
- Provide a high-level approach for how the incident response capability fits into the overall organization.
- Meet the unique requirements for the sytem, which relate to mission, size, structure, and functions.
- Provide metrics for measuring the incident response capability within the system.
- Define the resources and management support needed to effectively maintain and mature an incident response capability; and
- Ensure the incident response plan is reviewed and approved initially by NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements.

4.1.9 Maintenance

Table 4.1-9 summarizes the common and hybrid security control responsibilities for the MA family of controls. The detailed section that follows describes the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-9: MA Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
MA-1	System Maintenance Policy and Procedures	CSO, System Owners	Hybrid
MA-2	Controlled Maintenance	System Owners	System-specific
MA-2[2]	Record Content	System Owners	System-specific
MA-3	Maintenance Tools	System Owners	System-specific
MA-3[1]	Inspect Tools	System Owners	System-specific
MA-3[2]	Inspect Media	System Owners	System-specific
MA-3[3]	Unauthorized Removal	System Owners	System-specific
MA-4	Nonlocal Maintenance	System Owners	System-specific
MA-4[2]	Document Nonlocal Maintenance	System Owners	System-specific
MA-4[3]	Comparable Security / Sanitization	System Owners	System-specific

Control ID	Control Title	Provider(s)	Control Type
MA-5	Maintenance Personnel	System Owners	System-specific
MA-5[1]	Individuals Without Appropriate Access	System Owners	System-specific
MA-6	Timely Maintenance	System Owners	System-specific

4.1.9.1 MA-1 System Maintenance Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A system maintenance policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls;
- Reviews and updates the current:
  - System maintenance policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - System maintenance procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide system maintenance control policy, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific system maintenance procedures are developed, reviewed/updated, and maintained in accordance with NRC requirements.
- Ensure that system-specific system maintenance procedures facilitate the implementation of system maintenance policy.

4.1.10 Media Protection

Table 4.1-10 summarizes the common and hybrid security control responsibilities for the MP family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-10: MP Family Common and Hbrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
MP-1	Media Protection Policy and Procedures	CSO, System Owners	Hybrid
MP-2	Media Access	System Owners	System Specific
MP-3	Media Marking	System Owners	System Specific
MP-4	Media Storage	System Owners	System Specific
MP-5	Media Transport	System Owners	System Specific
MP-5[4]	Cryptographic Protection	System Owners	System Specific
MP-6	Media Sanitization	CSO, ADM, OIS , System Owners	Hybrid
MP-6[1]	Review / Approve / Track / Document / Verify	CSO, ADM, OIS, System Owners	Hybrid
MP-6[2]	Equipment Testing	CSO, ADM, OIS, System Owners	Hybrid
MP-6[3]	Nondestructive Techniques	CSO, System Owners	Hybrid
MP-7	Media Use	CSO, System Owners	Hybrid
MP-7[1]	Prohibit Use Without Owner	System Owners	System Specific

4.1.10.1 MP-1 Media Protection Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A media protection policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the media protection policy and associated media protection controls;

- Reviews and updates the current:
  - Media protection policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Media protection procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide media protection control policy, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific media protection procedures are developed, reviewed/updated, and maintained in accordance with NRC requirements.
- Ensure that system-specific media protection procedures facilitate the implementation of media protection policy.

4.1.10.2 MP-6 Media Sanitization

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Sanitizes information system media prior to disposal, release out of organizational control, or release for reuse in accordance with CSO-STD-2004, “Electronic Media and Device Handling;” and
- Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Provider Responsibilities:

CSO must:

- Provide requirements for proper media sanitization.

ADM must:

- Sanitize safeguards information, digital and non-digital media, using NRC Chief Information Security Officer (CISO) authorized techniques and maintain records of the media serial number and date of sanitization.

- Sanitize classified information digital and non-digital media using the National Security Agency (NSA) authorized techniques and meeting NSA documentation requirements.

OIS must**:**

- Sanitize SUNSI digital media using NRC CISO authorized techniques and maintain records of the media serial number and date of sanitization.

System owners must:

- Ensure that media sanitization actions are tracked, documented, and verified in accordance with CSO-STD-2004.

4.1.10.2.1 MP-6[1] Review / Approve / Track / Document / Verify

This is a ***hybrid*** security control with responsibilities for **CSO**, **ADM**, **OIS**, and **system owners**.

Control Description:

The NRC reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Provider Responsibilities:

CSO must:

- Provide requirements for tracking, documenting and verifying media sanitization actions.

ADM must:

- Review, approve, track, document, and verify digital and non-digital media sanitization and disposal actions for SGI and classified information digital and non-digital media in accordance with CSO-STD-2004.

OIS must:

- Review, approve, track, document, and verify digital media sanitization and disposal actions for SUNSI digital media in accordance with CSO-STD-2004.

System owners must:

- Ensure that media sanitization actions are tracked, documented, and verified in accordance with CSO-STD-2004.

4.1.10.2.2 MP-6[2] Equipment Testing

This is a ***hybrid*** security control with responsibilities for **CSO**, **ADM**, **OIS**, and **system owners**.

Control Description:

The NRC tests sanitization equipment and procedures in accordance with CSO-STD-0020 to verify that the intended sanitization is being achieved.

Provider Responsibilities:

CSO must:

- Define the timeframe for testing media sanitization equipment and procedures.

ADM must:

- Test sanitization equipment and procedures in accordace with CSO-STD-2004 and other NRC requirements to verify that the intended sanitization for SGI and classified Information, digital and non-digital media, is being achieved.

OIS must**:**

- Test sanitization equipment and procedures in accordace with CSO-STD-2004 and other NRC requirements to verify that the intended sanitization for SUNSI digital media is being achieved.

System owners must:

- Ensure media sanitization equipment and procedures to verify correct performance is tested in accordance with CSO-STD-2004 and other NRC requirements.

4.1.10.2.3 MP-6[3] Nondestructive Techniques

This is a ***hybrid*** security control with responsibilities for **CSO** and **system owners**.

Control Description:

The NRC applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system.

Provider Responsibilities:

CSO must:

- Define circumstances requiring sanitization of portable storage devices in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that portable, removable storage devices are sanitized prior to connecting such devices to the system in accordance with CSO-STD-2004 and other NRC requirements.

4.1.10.2.4 MP-7 Media Use

This is a ***hybrid*** security control with responsibilities for **CSO** and **system owners**.

Control Description:

The NRC prohibits the use personally owned, removable media on information systems in accordance with "NRC Agency-wide Rules of Behavior for Authorized Computer Use" and CSO-STD-1004, "General Laptop Configuration Standard."

Provider Responsibilities:

CSO must:

- Provide media use policy for NRC systems.

System owners must:

- Enforce media use policy which prohibits the use of personally owned, removable media on information systems in accordance with "NRC Agency-wide Rules of Behavior for Authorized Computer Use" and CSO-STD-1004.

4.1.11 Physical and Environmental Protection

Table 4.1-11 summarizes the common and hybrid security control responsibilities for the PE protection family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-11: PE Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
PE-1	Physical and Environmental Protection and Procedures	CSO, ADM, System Owners	Hybrid
PE-2	Physical Access Authorizations	CSO, ADM, System Owners	Hybrid
PE-3	Physical Access Control	CSO, ADM, System Owners	Hybrid
PE-3[1]	Information System Access	ADM, System Owners	Hybrid
PE-4	Access Control for Transmission Medium	CSO, ADM, OIS, System Owners	Hybrid
PE-5	Access Control for Output Devices	ADM, System Owners	Hybrid
PE-6	Monitoring Physical Access	CSO, ADM, OIS, System Owners	Hybrid
PE-6[1]	Intrusion Alarms / Surveillance Equipment	ADM, System Owners	Hybrid
PE-6[4]	Monitoring Physical Access to Information Systems	ADM, OIS, System Owners	Hybrid

Control ID	Control Title	Provider(s)	Control Type
PE-8	Visitor Access Records	CSO, ADM, OIS, System Owners	Hybrid
PE-8[1]	Automated Records Maintenance / Review	ADM, System Owners	Hybrid
PE-9	Power Equipment and Cabling	ADM, System Owners	Hybrid
PE-10	Emergency Shutoff	CSO, ADM, System Owners	Hybrid
PE-11	Emergency Power	OIS, System Owners	Hybrid
PE-11[1]	Long-Term Alternate Power Supply – Minimal Operational Capability	ADM, System Owners	Hybrid
PE-12	Emergency Lighting	ADM, System Owners	Hybrid
PE-13	Fire Protection	ADM, System Owners	Hybrid
PE-13[1]	Detection Devices / Systems	CSO, ADM, System Owners	Hybrid
PE-13[2]	Suppression Devices / Systems	CSO, ADM, System Owners	Hybrid
PE-13[3]	Automatic Fire Suppression	ADM, System Owners	Hybrid
PE-14	Temperature and Humidity Controls	CSO, ADM, System Owners	Hybrid
PE-15	Water Damage Protection	ADM, OIS, System Owners	Hybrid
PE-15[1]	Automation Support	CSO, ADM, System Owners	Hybrid
PE-16	Delivery and Removal	System Owners	System Specific
PE-17	Alternate Work Site	System Owners	System Specific
PE-18	Location of Information System Components	System Owners	System Specific

4.1.11.1 PE-1 Physical and Environmental Protection Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and

  - Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls;

- Reviews and updates the current:

  - Physical and environmental protection policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Physical and environmental protection procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide physical and environmental protection policy as it applies to NRC systems, define the frequency for reviews and updates, and distribute to NRC users.

ADM must:

- Provide physical security policy, requirements and procedures to protect personnel, SUNSI, SGI, classified information, facilities, and NRC assets.

System owners must:

- Ensure that system-specific physical and environment protection procedures are developed, reviewed/updated and maintained in accordance with NRC requirements to include NRC systems residing at non-NRC facilities.
- Ensure that system-specific physical and environment protection procedures facilitate the implementation of physical and environment protection policy.

4.1.11.2 PE-2 Physical Access Authorizations

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**.

Control Description:

The NRC:

- Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
- Issues authorization credentials for facility access;
- Reviews the access list detailing authorized facility access by individuals in accordance with CSO-STD-0020 and other NRC requirements; and
- Removes individuals from the facility access list when access is no longer required.

Provider Responsibilities:

CSO must:

- Define the frequency for reviewing the facility access list.

ADM must:

- Define publically accessible areas, issue authorization credentials for facility access, and keep current lists of personnel with authorized access to NRC facilities.
- Remove individuals from the facility access list when access is no longer required.

System owners must:

- Determine whether physical access is approved to the system and notify ADM to place the individual within the Physical Access Control System (PACS).
- Ensure the physical access list is reviewed and approved in accordance with CSO-STD-0020.
- Notify ADM when individuals need to be removed from the facility access list when access is no longer required.
- Ensure that system-specific policy, processes, and procedures are developed, reviewed, and maintained for enforcing authorized access to non-NRC facilities where NRC systems reside.

4.1.11.3 PE-3 Physical Access Control

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**.

Control Description:

The NRC:

- Enforces physical access authorizations at all NRC-defined entry/exit points to the facility where the information system resides in accordance with CSO-STD-0020 and other NRC requirements:
  - Verifying individual access authorizations before granting access to the facility; and
  - Controlling ingress/egress to the facility using NRC-defined physical access control systems/devices in accordance with CSO-STD-0020 and other NRC requirements;
- Maintains physical access audit logs for NRC-defined entry/exit points;
- Provides NRC-defined security safeguards to control access to areas within the facility officially designated as publicly accessible;

- Escorts visitors and monitors visitor activity within the NRC-controlled space in accordance with CSO-STD-0020 and other NRC requirements;
- Secures keys, combinations, and other physical access devices;
- Inventories NRC-defined physical access devices in accordance with CSO-STD-0020 and other NRC requirements; and
- Changes combinations and keys and physical access devices within the NRC-defined frequency and/or when keys or physical access devices are lost, combinations are compromised, or individuals are transferred or terminated in accordance with MD 12.1, "NRC Facility Security Program."

Provider Responsibilities:

CSO must:

- Define the appropriate physical access control systems/devices that control ingress/egress to the facility.

ADM must:

- Enforce physical access authorizations for all physical access points into NRC facilities, including designated entry/exit points to the facility where the system resides using card readers and guards.
- Control ingress/egress to the facility using NRC-defined physical access control systems/devices.
- Ensure that visitors entering NRC facilities have been issued appropriate visitor badges, escorted while present in the building, and monitored in accordance with CSO-STD-0020 and other NRC requirements.
- Ensure combinations and keys are changed when keys are lost, combinations are compromised, or individuals are transferred or terminated.

System owners must:

- Determine whether physical access is approved to the location where the NRC system resides.
- Ensure that visitors are escorted and monitored in accordance with CSO-STD-0020 and other NRC requirements.
- Notify ADM when keys are lost, combinations are compromised, or individuals are transferred or terminated**.**
- Ensure that physical access control to non-NRC facilities is enforced where NRC systems reside in accordance with CSO-STD-0020 and other NRC requirements.

4.1.11.3.1 PE-3[1] Information System Access

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**.

Control Description:

The NRC:

- Enforces physical access authorizations to the system in addition to the physical access controls for the facility where there is a concentration of information system components (i.e., server rooms, media storage areas, wiring closets, and data and communications centers).

Provider Responsibilities:

ADM must:

- Enforce physical access authorizations where there is a concentration of information system components (i.e., server rooms, media storage areas, wiring closets, and data centers).

System owners must:

- Determine whether physical access is approved to the location where there is a concentration of system components (i.e., server rooms, media storage areas, wiring closets, and data centers).
- Enforce physical access control where there is a concentration of system components (i.e., server rooms, media storage areas, wiring closets, and data centers) in non-NRC facilities where NRC systems reside in accordance with NRC requirements.

4.1.11.4 PE-4 Access Control for Transmission Medium

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, **OIS**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC controls physical access to NRC-defined information system distribution and transmission lines within NRC facilities in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define the proper safeguards for controlling physical acess to information system distribution and transmission lines.

ADM must:

- Control physical access to NRC system distribution and transmission lines within NRC facilities in accordance with CSO-STD-0020 and other NRC requirements.

OIS must:

- Control physical access to NRC system distribution and transmission lines located inside of the NRC data centers.

System owners must:

- Ensure that physical access to transmission medium for the system is controlled using proper safeguards in non-NRC facilities where NRC systems reside in accordance with CSO-STD-0020 and other NRC requirements.

4.1.11.5 PE-5 Access Control for Output Devices

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Provider Responsibilities:

ADM must:

- Enforce physical access restriction to output devices throughout NRC facilities to prevent unauthorized individuals from obtaining the output.

System owners must:

- Ensure physical access to system-specific output devices is controlled to prevent unauthorized individuals from obtaining the output in non-NRC facilities where NRC systems reside.

4.1.11.6 PE-6 Monitoring Physical Access

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, **OIS**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC:

- Monitors physical access to the facility where the NRC system resides to detect and respond to physical security incidents;
- Reviews physical access logs in accordance with CSO-STD-0020; and
- Coordinates results of reviews and investigations in accordance with CSO-STD-0020.

Provider Responsibilities:

CSO must:

- Define the frequency for reviewing physical access logs.

ADM must:

- Provide physical access monitoring through detection and prevention systems including NRC guards, Homeland Security Presidential Directive (HSPD)-12 badge readers, closed-circuit surveillance cameras and a real-time intrusion alarm system for NRC facilities.
- Review physical access logs in accordance with CSO-STD-0020 and other NRC requirements.
- Report suspicious physical access activities in accordance with MD 12.5, CSO-STD-0020, and other NRC requirements.

OIS must:

- Monitor and review physical access logs to the data centers where the NRC system resides.
- Report suspicious physical access activities in accordance with MD 12.5, CSO-STD-0020, and other NRC requirements.

System owners must:

- Ensure that physical access to the facility where the system resides is monitored and physical access logs are reviewed daily to detect and respond to physical security incidents to NRC systems that reside in non-NRC facilities.
- Ensure that suspicious physical access activities for NRC systems that reside in non-NRC facilities are reported in accordance with CSO-STD-0020.

4.1.11.6.1 PE-6[1] Intrusion Alarms / Surveillance Equipment

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC monitors real-time physical intrusion alarms and surveillance equipment.

Provider Responsibilities:

ADM must:

- Provide real-time physical intrusion alarms and surveillance equipment for systems hosted in NRC facilities.

System owners must:

- Ensure that real-time physical intrusion alarms and surveillance equipment is provided for NRC systems hosted in non-NRC facilities.

4.1.11.6.2 PE-6[4] Monitoring Physical Access to Information Systems

This is a ***hybrid*** security control with responsibilities for the **ADM**, **OIS**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC monitors physical access to the system in addition to the physical access monitoring of the facility containing one or more components of the information system in accordance with MD 12.1, “NRC Facility Security Plan,” and other NRC requirements.

Provider Responsibilities:

ADM must:

- Monitor physical access to the system in addition to the physical access monitoring of the facility containing one or more components of the information system in accordance with MD 12.1 and other NRC requirements.

OIS must:

- Ensure that physical access for NRC data centers is monitored to information systems.

System owners must:

- Ensure that physical access to information systems is monitored in addition to the physical access monitoring of the facility where there is a concentration of information system components (i.e., server rooms, media storage areas, wiring closets, and data centers) for NRC systems that reside in non-NRC facilities.

4.1.11.7 PE-8 Visitor Access Records

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Maintains visitor access records to the facility where the information system resides in accordance with CSO-STD-0020 and other NRC requirements; and
- Reviews visitor access records in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define the timeframe for maintaining visitor access records.

ADM must:

- Administer the visitor access control program and maintain and review visitor access records for visitors entering and exiting NRC facilities.

OIS must:

- Maintain and review visitor records for visitors entering and exiting NRC data centers.

System owners must:

- Ensure that visitor access records are maintained and reviewed for NRC systems that reside in non-NRC facilities in accordance with CSO-STD-0020 and other NRC requirements.

4.1.11.7.1 PE-8[1] Automated Records Maintenance / Review

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC employs automated mechanisms to facilitate the maintenance and review of visitor access records.

Provider Responsibilities:

ADM must:

- Employ automated mechanisms to facilitate the maintenance and review of visitor access records to NRC facilities.

System owners must:

- Ensure that automated mechanisms to facilitate the maintenance and review of visitor access records are employed for NRC systems that reside in non-NRC facilities.

4.1.11.8 PE-9 Power Equipment and Cabling

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC protects power equipment and power cabling for the information system from damage and destruction.

Provider Responsibilities:

ADM must:

- Ensure that power equipment and cabling is protected from damage and destruction in accordance with NRC requirements.

System owners must:

- Ensure that power equipment and power cabling for the system is protected from damage and destruction for NRC systems hosted in non-NRC facilities.

4.1.11.9 PE-10 Emergency Shutoff

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC:

- Provides the capability of shutting off power to the information system or individual system components in emergency situations;
- Places emergency shutoff switches or devices in accordance with CSO-STD-0020 and other NRC requirements to facilitate safe and easy access for personnel; and
- Protects emergency power shutoff capability from unauthorized activation.

Provider Responsibilities:

CSO must:

- Define the types of locations where emergency shutoff switches or devices should be placed to facilitate safe and easy access for personnel.

ADM must:

- Provide the capability of shutting off power to the information system or individual system components in emergency situations.
- Place emergency shutoff switches or devices in accordance with CSO-STD-0020 and other NRC requirements to facilitate safe and easy access for personnel.
- Protect emergency power shutoff capability from unauthorized activation.

System owners must:

- Ensure that capability of shutting off power to the system or system components in emergency situations is provided for NRC systems that reside in non-NRC facilities.
- Ensure that emergency shutoff switches or devices are placed in accordance with CSO-STD-0020 and other NRC requirements for NRC systems that reside in non-NRC facilities to facilitate safe and easy access for personnel; and
- Ensure that emergency power shutoff capability from unauthorized activation is provided for NRC systems that reside in non-NRC facilities.

4.1.11.10 PE-11 Emergency Power

This is a ***hybrid*** security control with responsibilities for the **OIS** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC provides a short-term (e.g., 30-45 minutes) uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Provider Responsibilities:

OIS must:

- Provide an uninterruptible power supply for those NRC systems hosted in NRC data centers.

System owners must:

- Ensure that emergency shutoff capabilities are provided for NRC systems hosted in non-NRC facilities.

4.1.11.10.1 PE-11[1] Long-Term Alternate Power Supply – Minimal Operational Capability

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Provider Responsibilities:

ADM must:

- Provide a long-term alternate power supply for NRC systems hosted in NRC facilities.

System owners must:

- Ensure that a long-term alternate power supply for NRC systems hosted in non-NRC facilities is provided.

4.1.11.11 PE-12 Emergency Lighting

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Provider Responsibilities:

ADM must:

- Provide automatic emergency lighting for NRC facilities that activate in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.

System owners must:

- Ensure that automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility for NRC systems hosted in non-NRC facilities is provided.

4.1.11.12 PE-13 Fire Protection

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Provider Responsibilities:

ADM must:

- Provide fire suppression and detection devices/systems for NRC system that are installed and supported by an independent energy source in NRC facilities.

System owners must:

- Ensure that fire suppression and detection devices/systems that are supported by an independent energy source are provided and maintained for NRC systems hosted in non-NRC facilities.

4.1.11.12.1 PE-13[1] Detection Devices / Systems

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC employs fire detection devices/systems for the information system that activate automatically and notify NRC-defined personnel or roles and NRC-defined emergency responders in the event of a fire in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define appropriate personnel or roles to be notified automatically in the event of a fire.

ADM must:

- Provide fire detection devices/systems in NRC facilities that activate automatically and notify NRC-defined personnel or roles and NRC-defined emergency responders in the event of a fire in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that fire detection devices/systems that activate automatically and notify pre-defined personnel or roles and emergency responders in the event of a fire for NRC systems hosted in non-NRC facilities are provided.

4.1.11.12.2 PE-13[2] Suppression Devices / Systems

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC employs fire suppression devices/systems for the information system that provide automatic notification of any activation in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define appropriate personnel or roles to be notified automatically of any activation.

ADM must:

- Provide fire suppression devices and systems in NRC facilities that provide automatic notification of any activation in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that fire suppression devices and systems that provide automatic notification of any activation are provided for NRC systems hosted in non-NRC facilities.

4.1.11.12.3 PE-13[3] Automatic Fire Suppression

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Provider Responsibilities:

ADM must:

- Provide an automatic fire suppression capability in NRC facilities for the system when the facility is not staffed on a continuous basis.

System owners must:

- Ensure that an automatic fire suppression capability is provided for NRC systems hosted in non-NRC facilities when the facility is not staffed on a continuous basis.

4.1.11.13 PE-14 Temperature and Humidity Controls

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC:

- Maintains temperature and humidity levels within the facility where the information system resides in accordance with CSO-STD-0020 and other NRC requirements; and
- Monitors temperature and humidity levels in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define appropriate temperature and humidity levels.
- Define the frequency for monitoring temperature and humidity levels.

ADM must:

- Monitor and maintain temperature and humidity levels within the facility where the information system resides in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that temperature and humidity levels are monitored and maintained for NRC systems hosted in non-NRC facilities in accordance with CSO-STD-0020 and other NRC requirements.

4.1.11.14 PE-15 Water Damage Protection

This is a ***hybrid*** security control with responsibilities for the **ADM**, **OIS**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Provider Responsibilities:

ADM must:

- Protect NRC facilities from water damage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

OIS must:

- Ensure that key personnel within NRC data centers know where master shutoff valves are located in case of a water leak.

System owners must:

- Ensure that NRC systems hosted in non-NRC facilities are protected from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

4.1.11.14.1 PE-15[1] Automation Support

This is a ***hybrid*** security control with responsibilities for **CSO**, **ADM**, and **system owners**. Systems hosted inside of NRC-facilities may inherit this control.

Control Description:

The NRC employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define appropriate personnel or roles to alert in case water is detected in the vicinity of the information system.

ADM must:

- Provide automated mechanisms to detect the presence of water in the vicinity of the information system and alerts NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that automatic mechanisms that will shutoff water to protect the systems in the event of a leak are employed for NRC systems hosted in non-NRC facilities.

4.1.12 Planning

Table 4.1-12 summarizes the common and hybrid security control responsibilities for the PL family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-12: PL Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
PL-1	Security Planning and Policy Procedures	CSO, System Owners	Hybrid
PL-2	System Security Plan	System Owners	System Specific
PL-2[3]	Coordinate with Other Organizational Entities	System Owners	System Specific
PL-4	Rules of Behavior	CSO, System Owners	Hybrid
PL-4[1]	Social Media and Networking Restrictions	CSO, System Owners	Hybrid
PL-8	Information Security Architecture	System Owners	System Specific

4.1.12.1 PL-1 Security Planning Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A security planning policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the security planning policy and associated security planning controls;
- Reviews and updates the current:
  - Security planning policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Security planning procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide security planning policy, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific security planning procedures are developed, reviewed, and maintained in accordance with NRC requirements.
- Ensure that system-specific security planning procedures facilitate the implementation of security planning policy.

4.1.12.2 PL-4 Rules of Behavior

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Establishes and makes readily available to individuals requiring access to the information system, the rules that describe the responsibilities and expected behavior with regard to information and information system usage;
- 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 system;
- Reviews and updates the rules of behavior in accordance with CSO-STD-0020 and other NRC requirements; and
- 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.

Provider Responsibilities:

CSO must:

- Establish and make readily available to individuals requiring access to the information system, the rules (e.g., “Agency-wide Rules of Behavior for Authorized Computer Use”). That describe the responsibilities and expected behavior with regard to information and information system usage.
- Receive a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior.
- Review and update the rules of behavior in accordance with CSO-STD-0020 and other NRC requirements.

- Require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

System owners must:

- Determine if system-specific rules of behavior are necessary.
- Ensure that system-specific rules of behavior are developed, maintained, and signed by users for the specific system environment describing the responsibilities and expected behavior with regard to information and information system usage.
- Review and update system-specific rules of behavior in accordance with CSO-STD-0020 and other NRC requirements.
- Require individuals who have signed a previous version of the system-specific rules of behavior to read and re-sign when the rules of behavior are revised/updated.

4.1.12.2.1 PL-4[1] Social Media and Networking Restrictions

This is a ***hybrid*** security control with responsibilities for **CSO** and **system owners**.

Control Description:

The NRC includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Provider Responsibilities:

CSO must:

- Include in the rules of behavior (e.g., “Agency-wide Rules of Behavior for Authorized Computer Use”) explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

System owners must:

- Ensure that system-specific rules of behavior includes explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

4.1.13 Personnel Security

Table 4.1-13 summarizes the common and hybrid security control responsibilities for the PS family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-13: PS Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
PS-1	Personnel Security Policy and Procedures	ADM	Common
PS-2	Position Risk Designation	OEDO, ADM, OCHCO	Common
PS-3	Personnel Screening	ADM, System Owners	Hybrid
PS-4	Personnel Termination	OCHCO, System Owners	Hybrid
PS-4[2]	Automated Notification	OCHCO	Common
PS-5	Personnel Transfer	OCHCO, System Owners	Hybrid
PS-6	Access Agreements	CSO, System Owners	Hybrid
PS-7	Third-Party Personnel Security	CSO, ADM, System Owners	Hybrid
PS-8	Personnel Sanctions	ADM, OCHCO	Common

4.1.13.1 PS-1 Personnel Security Policy and Procedures

This is a ***common*** security control with responsibilities for the **ADM**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls;
- Reviews and updates the current:
  - Personnel security policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Personnel security procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

ADM must:

- Develop, document, and administer policies and procedures for the NRC personnel security program that are in accordance with MD 12.3, “NRC Personnel Security Program,” and oversee the NRC personnel security program.

4.1.13.2 PS-2 Position Risk Designation

This is a ***common*** security control with responsibilities for the **OEDO**, **ADM**, and **OCHCO**.

Control Description:

The NRC:

- Assigns a risk designation to all organizational positions;
- Establishes screening criteria for individuals filling those positions; and
- Reviews and updates position risk designations in accordance with MD 12.3.

Provider Responsibilities:

OEDO must:

- Approve the sensitivity criteria to be used in determining whether individual contractor employees require IT Level I or Level II approval for access to NRC IT systems or access to sensitive information.

ADM must:

- Define position sensitivity criteria and assign risk designation for organizational positions and associated clearance levels and conduct activities accordingly.

OCHCO must:

- Determine, assign, and perform position and associated screening criteria for NRC employees and applicants for employment.

4.1.13.3 PS-3 Personnel Screening

This is a ***hybrid*** security control with responsibilities for the **ADM** and **system owners**.

Control Description:

The NRC:

- Screens individuals prior to authorizing access to the information system; and

- Rescreens individuals according to MD 12.3 requiring rescreening and, where rescreening is so indicated, defines the frequency of such rescreening.

Provider Responsibilities:

ADM must:

- Conduct personnel screening interviews, clearance activities, background checks, and authorization requests on behalf of system owners for all NRC personnel prior to facilities and system access.
- Rescreen individuals according to MD 12.3 requiring rescreening (e.g., change in security clearance level) and, where rescreening is so indicated, and define the frequency of such rescreening.

System owners must:

- Ensure that personnel requesting access to NRC systems have been cleared and authorized prior to system access.
- Ensure that personnel are rescreened in accordance with MD 12.3.

4.1.13.4 PS-4 Personnel Termination

This is a ***hybrid*** security control with responsibilities for the **OCHCO** and **system owners**.

Control Description:

The NRC, upon termination of individual employment for NRC staff and contractors:

- Disables information system access in accordance with CSO-STD-0020 and other NRC requirements;
- Terminates/revokes any authenticators/credentials associated with the individual;
- Conducts exit interviews;
- Retrieves all security-related system NRC information system-related property;
- Retains access to organizational information and information systems formerly controlled by terminated individual; and
- Notifies NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

OCHCO must:

- Notify system owners of NRC staff and contractor termination at least 3 calendar days prior to the last day of employment and indicate whether or not the termination is voluntary.

System owners must ensure the following activities are conducted:

- Information system access is disabled on the last day of employment for voluntary terminations and prior to user notification for involuntary terminations.
- Any authenticators/credentials associated with the individual are terminated/revoked.
- Exit interviews are conducted that include a discussion of security topics defined in NRC Form 136, "Security Termination Statement," to obtain important system information from the employee and to ensure access to information and IT systems is not disrupted.
- All security-related system property (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, mobile devices and building passes) are retrieved.
- Ensure that appropriate personnel have access to official records created by the transferring or terminated employee that are stored on organizational IT systems.

4.1.13.4.1 PS-4[2] Automated Notification

This is a ***common*** security control with responsibilities for **OCHCO**.

Control Description:

The NRC employs automated mechanisms to notify system owners of NRC staff and contractor terminations and transfers.

Provider Responsibilities:

OCHCO must:

- Employ automated mechanisms (e.g., telephony, email) to notify system owners of NRC staff and contractor terminations and transfers.

4.1.13.5 PS-5 Personnel Transfer

This is a ***hybrid*** security control with responsibilities for the **OCHCO**, and **system owners**.

Control Description:

The NRC:

- Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when NRC staff and contractors are reassigned or transferred to other positions within the NRC;
- Initiates NRC-defined transfer or reassignment actions in accordance with CSO-STD-0020 and other NRC requirements following the formal transfer action;
- Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

- Notifies NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

OCHCO must:

- Notify the system owner at least 5 calendar days prior to the transfer date.

System owners must:

- Ensure that existing facility access authorizations are reviewed and access is removed if no longer required in the new position.
- Ensure keys/building passes are collected when NRC staff and contractors no longer require access to those locations to perform new position functions.
- Ensure facility access codes are modified when NRC staff and contractors no longer require access to those locations to perform new position functions.
- Ensure identification cards are collected when NRC staff and contractors no longer require them to perform new position functions.
- Ensure existing system access authorizations are reviewed and access is removed when no longer required in the new position.
- Ensure mobile devices are collected when NRC staff and contractors no longer require in the new position.
- Ensure old accounts are disabled when no longer required to perform new position functions.

4.1.13.6 PS-6 Access Agreements

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops and documents access agreements for NRC information systems;
- Reviews and updates the access agreements in accordance with CSO-STD-0020 and other NRC requirements; and
- Ensures that individuals requiring access to NRC information and information systems:
  - Sign appropriate access agreements prior to being granted access; and
  - Re-sign access agreements to maintain access to NRC information systems when access agreements have been updated in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop and document agency-wide access agreements (e.g., “Agency-wide Rules of Behavior for Authorized Computer Use”) which define expected behavior with regard to information and system usage and defines the frequency of review and updates for access agreements.

System owners must:

- Develop and document system-specific access agreements.
- Ensure that system-specific access agreements are signed prior to being granted access and re-signed when access agreements have been updated.
- Ensure that system-specific access agreements are reviewed and updated in accordance with CSO-STD-0020 and other NRC requirements.
- Ensure that system users acknowledge and sign all agency-wide access agreements.

4.1.13.7 PS-7 Third-Party Personnel Security

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**.

Control Description:

The NRC:

- Establishes personnel security requirements including security roles and responsibilities for third-party providers;
- Requires third-party providers to comply with personnel security policies and procedures established by NRC;
- Documents personnel security requirements;
- Requires third-party providers to notify NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements of any personnel transfers or terminations of third-party personnel who possess NRC credentials and/or badges, or who have information system privileges in accordance with CSO-STD-0020 and other NRC requirements; and
- Monitors provider compliance.

Provider Responsibilities:

CSO must:

- Define the timeframe and appropriate NRC personnel or roles to notify of any personnel transfers or terminations of third-party personnel who possess NRC credentials and/or badges.

ADM must:

- Establish personnel security requirements including security roles and responsibilities for third-party providers.
- Require third-party providers to comply with personnel security policies and procedures established by NRC.
- Document personnel security requirements.
- Require third-party providers to notify NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements of any personnel transfers or terminations of third-party personnel who possess NRC credentials and/or badges, or who have information system privileges in accordance with CSO-STD-0020 and other NRC requirements.
- Monitor provider compliance.

System owners must:

- Ensure that third-party providers comply with personnel security policies and procedures established by NRC.
- Ensure that the Contracting Officers Representative (COR) is notified of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges in accordance with CSO-STD-0020 and other NRC requirements.
- Monitor third-party provider compliance.

4.1.13.8 PS-8 Personnel Sanctions

This is a ***common*** security control with responsibilities for the **ADM** and **OCHCO**.

Control Description:

The NRC:

- Employs a formal sanctions process for NRC staff and contractors failing to comply with established information security policies and procedures; and
- Notifies NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Provider Responsibilities:

ADM must:

- Employ the formal sanctions for NRC staff and contractors failing to comply with established information security policies and procedures.

OCHCO must:

- Notify NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

4.1.14 Risk Assessment

Table 4.1-14 summarizes the common and hybrid security control responsibilities for the RA family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-14: RA Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
RA-1	Risk Assessment Policy and Procedures	CSO, System Owners	Hybrid
RA-2	Security Categorization	CSO, System Owners	Hybrid
RA-3	Risk Assessment	System Owners	System Specific
RA-5	Vulnerability Scanning	CSO, OIS, System Owners	Hybrid
RA-5[1]	Update Tool Capability	OIS, System Owners	Hybrid
RA-5[2]	Update by Frequency / Prior To New Scan / When Identified	OIS, System Owners	Hybrid
RA-5[4]	Discoverable Information	CSO, OIS, System Owners	Hybrid
RA-5[5]	Privileged Access	OIS, System Owners	Hybrid

4.1.14.1 RA-1 Risk Assessment Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A risk assessment policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among organizational entities, and compliance; and
  - Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls;

- Reviews and updates the current:
  - Risk assessment policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - Risk assessment procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide risk assessment policy, define the frequency for reviews and updates, and distribute to NRC users.

System owners must:

- Ensure that system-specific risk assessment procedures are developed, reviewed and maintained in accordance with NRC requirements.
- Ensure that system-specific risk assessment procedures facilitate the implementation of risk assessment policy.

4.1.14.2 RA-2 Security Categorization

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
- Ensures that the security categorization is reviewed and approved by the authorizing official or authorizing official designated representative.

Provider Responsibilities:

CSO must:

- Review and approve the security categorization.

System owners must:

- Categorize information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Document the security categorization results (including supporting rationale) in the security plan for the information system; and
- Submit the security categorization for review and approval by the authorizing official or authorizing official designated representative.

4.1.14.3 RA-5 Vulnerability Scanning

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Scans for vulnerabilities in the information system and hosted applications within the NRC-defined frequency and/or randomly in accordance with CSO-STD-0020 and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting checklists and test procedures; and
  - Measuring vulnerability impact;
- Analyzes vulnerability scan reports and results from security control assessments;
- Remediates legitimate vulnerabilities in accordance with CSO-STD-0020 and other NRC requirements and assessment of risk; and
- Shares information obtained from the vulnerability scanning process and security control assessments in accordance with CSO-STD-0020 and other NRC requirements to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Provider Responsibilities:

CSO must:

- Provide policy and requirements for system owners, identify approved scan tools, frequency for conducting scanning, vulnerability remediation timeframes, and reporting requirements.

OIS must:

- Scan for vulnerabilities in the information system and hosted applications for NRC systems that are part of the NRC managed networks in accordance with CSO-STD-0020 and other NRC requirements and when new vulnerabilities potentially affecting the system/applications are identified and reported.
- Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting checklists and test procedures; and
  - Measuring vulnerability impact.
- Analyze vulnerability scan reports and results from security control assessments.
- Share information obtained from the vulnerability scanning process and security control assessments in accordance with CSO-STD-0020 and other NRC requirements to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
- Provide each system ISSO with access to vulnerability scanning results within the Agency's vulnerability scanning tool.

System owners must:

- Ensure the system is scanned for vulnerabilities in accordance with CSO-STD-0020 and other NRC requirements and when new vulnerabilities potentially affecting the system/applications are identified and reported.
- Ensure that vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting checklists and test procedures; and
  - Measuring vulnerability impact.
- Analyze vulnerability scan reports and results from security control assessments.
- Remediate, (i.e., mitigate, obtain a deviation for) legitimate vulnerabilities in accordance with CSO-STD-0020 and other NRC requirements and assessment of risk.
- Share information obtained from the vulnerability scanning process and security control assessments in accordance with CSO-STD-0020 and other NRC requirements to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

4.1.14.3.1 RA-5[1] Update Tool Capability

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC employs vulnerability-scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Provider Responsibilities:

OIS must:

- Provide an enterprise-wide vulnerability scanning tool that has the capability to readily update system vulnerabilities to be scanned as new vulnerabilities are discovered for NRC systems that are part of the NRC managed networks.

System owners must:

- Ensure the system is scanned with a vulnerability-scanning tool that has the capability to readily update system vulnerabilities to be scanned as new vulnerabilities are discovered if not part of the enterprise-wide vulnerability-scanning tool.

4.1.14.3.2 RA-5[2] Update by Frequency / Prior To New Scan / When Identified

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC updates the list of system vulnerabilities scanned in accordance with CSO-STD-0020 prior to a new scan and when new vulnerabilities are identified and reported.

Provider Responsibilities:

OIS must:

- Provide an enterprise-wide vulnerability scanning tool that updates, in accordance with CSO-STD-0020 and other NRC requirements, the list of system vulnerabilities scanned prior to a new scan and when new vulnerabilities are identified and reported for NRC systems that are part of the NRC managed networks.

System owners must:

- Ensure the system is scanned with a vulnerability-scanning tool that updates system vulnerabilities to be scanned prior to a new scan and as new vulnerabilities are discovered.

4.1.14.3.3 RA-5[4] Discoverable Information

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC determines what information about the information system is discoverable by adversaries and subsequently takes corrective actions in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define the corrective actions for information about the system that is discoverable by adversaries.

OIS must:

- Determine what information about the system is discoverable by adversaries for NRC systems that are part of the NRC managed networks.
- Notify system owner of discoverable information by adversaries and collaborate on appropriate corrective actions in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Ensure that corrective actions are taken in accordance with CSO-STD-0020 and other NRC requirements for discoverable information by adversaries found during system scanning.

4.1.14.3.4 RA-5[5] Privileged Access

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC includes privileged access authorization for all host-based vulnerability scans for thorough vulnerability scanning.

Provider Responsibilities:

OIS must:

- Implement privileged access authorization for all host-based vulnerability scans for NRC systems that are part of the NRC managed networks.

System owners must:

- Ensure the system implements privileged access authorization for all host-based vulnerability scans.

4.1.15 System and Services Acquisition

Table 4.1-15 summarizes the common and hybrid security control responsibilities for the SA family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-15: SA Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
SA-1	System and Services Acquisition Policy and Procedures	CSO, ADM, System Owners	Hybrid
SA-2	Allocation of Resources	System Owners	System Specific
SA-3	System Development Life Cycle	System Owners	System Specific
SA-4	Acquisition Process	CSO, ADM, System Owners	Hybrid
SA-4[1]	Functional Properties of Security Controls	System Owners	System Specific
SA-4[2]	Implementation Information for Security Controls	System Owners	System Specific
SA-4[9]	Functions / Ports / Protocols / Services in use	System Owners	System Specific
SA-4[10]	Use of Approved PIV Products	System Owners	System Specific
SA-5	Information System Documentation	System Owners	System Specific
SA-8	Security Engineering Principles	System Owners	System Specific
SA-9	External Information System Services	System Owners	System Specific
SA-9[2]	Identification of Functions / Ports / Protocols / Services	System Owners	System Specific
SA-10	Developer Configuration Management	System Owners	System Specific
SA-11	Developer Security Testing and Evaluation	System Owners	System Specific
SA-12	Supply Chain Protection	System Owners	System Specific
SA-15	Development, Process, Standards, and Tools	System Owners	System Specific
SA-16	Developer-Provided Training	System Owners	System Specific
SA-17	Developer Security Architecture and Design	System Owners	System Specific

4.1.15.1 SA-1 System and Services Acquisition Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls;
- Reviews and updates the current:
  - System and services acquisition policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - System and services acquisition procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide system and services acquisition policy as it applies to NRC systems, define the frequency for reviews and updates, and distribute to NRC-defined users.

ADM must:

- Document, review, and maintain system and services acquisition policy for NRC within MD 11.1, “NRC Acquisition of Supplies and Services.”

System owners must:

- Ensure that system-specific system and services acquisition procedures are developed, reviewed and maintained for the systems in accordance with NRC requirements.
- Ensure that system-specific system and services acquisition procedures facilitate the implementation of system and services acquisition policy.

4.1.15.2 SA-4 Acquisition Process

This is a ***hybrid*** security control with responsibilities for the **CSO**, **ADM**, and **system owners**.

Control Description:

The NRC includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

- Security functional requirements;
- Security strength requirements;
- Security assurance requirements;
- Security-related documentation requirements;
- Requirements for protecting security-related documentation;
- Description of the information system development environment and environment in which the system is intended to operate; and
- Acceptance criteria.

Provider Responsibilities:

CSO must:

- Provide policy and guidance for IT cybersecurity requirements (e.g., security documentation, vulnerability scanning, to include development environment and environment in which the system is intended to operate) for NRC IT contracts.

ADM must:

- Provide policy for acquisition contracts in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

System owners must:

- Ensure that all system-specific contracts and services include the requirements listed below in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
  - Security functional requirements;
  - Security strength requirements;
  - Security assurance requirements;
  - Security-related documentation requirements;
  - Requirements for protecting security-related documentation;

- Description of the information system development environment and environment in which the system is intended to operate; and
- Acceptance criteria.

4.1.16 System and Communications Protections

Table 4.1-16 summarizes the common and hybrid security control responsibilities for the SC family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-16: SC Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
SC-1	System and Communications Protection Policy and Procedures	CSO, System Owners	Hybrid
SC-2	Application Partitioning	System Owners	System Specific
SC-3	Security Function Isolation	System Owners	System Specific
SC-4	Information in Shared Resources	System Owners	System Specific
SC-5	Denial of Service Protection	CSO, OIS, System Owners	Hybrid
SC-7	Boundary Protection	CSO, OIS, System Owners	Hybrid
SC-7[3]	Access Points	OIS, System Owners	Hybrid
SC-7[4]	External Telecommunications Services	CSO, OIS, System Owners	Hybrid
SC-7[5]	Deny By Default / Allow By Exception	OIS, System Owners	Hybrid
SC-7[7]	Prevent Split Tunneling for Remote Devices	OIS, System Owners	Hybrid
SC-7[8]	Route Traffic to Authenticated Proxy Servers	CSO, OIS, System Owners	Hybrid
SC-7[18]	Fail Secure	OIS, System Owners	Hybrid
SC-7[21]	Isolation of Information System Components	CSO, OIS, System Owners	Hybrid
SC-8	Transmission Confidentiality and Integrity	System Owners	System Specific
SC-8[1]	Cryptographic or Alternate Physical Protections	System Owners	System Specific
SC-10	Network Disconnect	CSO, OIS, System Owners	Hybrid
SC-12	Cryptographic Key Establishment and Management	System Owners	System Specific
SC-12[1]	Availability	System Owners	System Specific
SC-13	Cryptographic Protection	System Owners	System Specific
SC-15	Collaborative Computing Devices	System Owners	System Specific

Control ID	Control Title	Provider(s)	Control Type
SC-17	Public Key Infrastructure Certificates	CSO, OIS, System Owners	Hybrid
SC-18	Mobile Code	CSO, OIS, System Owners	Hybrid
SC-19	Voice Over Internet Protocol	CSO, System Owners	Hybrid
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	OIS, System Owners	Hybrid
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	OIS, System Owners	Hybrid
SC-22	Architecture and Provisioning for Name / Address Resolution Service	OIS, System Owners	Hybrid
SC-23	Session Authenticity	System Owners	System Specific
SC-24	Fail in Know State	System Owners	System Specific
SC-28	Protection of Information at Rest	System Owners	System Specific
SC-39	Process Isolation	System Owners	System Specific

4.1.16.1 SC-1 System and Communications Protection Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A system and communications protection policy that addresses purpose, scope, roles, responsibilities, organization-defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls;
- Reviews and updates the current:
  - System and communications protection policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - System and communications protection procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide system and communications protection policy and requirements as it applies to NRC systems and distribute to NRC users.

System owners must:

- Ensure that system-specific system and communications protection policies and procedures are developed, reviewed/updated and maintained in accordance with NRC requirements.
- Ensure that system-specific system and communications protection procedures facilitate the implementation of system and communications protection policy.

4.1.16.2 SC-5 Denial of Service Protection

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC protects against or limits the effects of denial of service (DoS) attacks in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must**:**

- Define the types of DoS attacks and the security safeguards that must be implemented to protect against or limit the effects of DoS attacks.

OIS must:

- Provide DoS protection for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure the information system is protected against or limited to the effects of DoS attacks.

4.1.16.3 SC-7 Boundary Protection

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system as defined in CSO-STD-4000, “Network Infrastructure Standard;”
- Implements subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and
- Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Provider Responsibilities:

CSO must:

- Provide requirements for controlling communications through managed interfaces and subnetwork requirements for NRC systems.

OIS must:

- Monitor and control communications at the external boundary of the system and at key internal boundaries for NRC systems connected to the NRC managed networks;
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and
- Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

System owners must:

- Ensure that communications at the external boundary of the system and at key internal boundaries within the system are monitored and controlled;
- Ensure that subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks are implemented; and
- Ensure that external networks or information systems are connected only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

4.1.16.3.1 SC-7[3] Access Points

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC limits the number of external network connections to the information system.

Provider Responsibilities:

OIS must:

- Limit the number of external network connections to NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that the number of external network connections for the system is limited in accordance with NRC requirements.

4.1.16.3.2 SC-7[4] External Telecommunications Services

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
- Reviews exceptions to the traffic flow policy in accordance with CSO-STD-0020 and removes exceptions that are no longer supported by an explicit mission/business need.

Provider Responsibilities:

CSO must:

- Define the required timeframe for reviewing exceptions to the traffic flow policy.

OIS must:

- Provide external telecommunications services to NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that a managed interface for each external telecommunication service is implemented for the system.
- Ensure that a traffic flow policy for each managed interface is established.
- Ensure that the confidentiality and integrity of the information being transmitted across each interface is protected.
- Ensure that each exception to the traffic flow policy is documented with a supporting mission/business need and duration of that need.
- Ensure that exceptions to the traffic flow policy are reviewed in accordance with CSO-STD-0020 and other NRC requirements and that exceptions are removed that are no longer supported by an explicit mission/business need.

4.1.16.3.3 SC-7[5] Deny By Default / Allow by Exception

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC denies network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny-all, permit-by-exception).

Provider Responsibilities:

OIS must:

- Deny network communications traffic at managed interfaces by default and allows network communications traffic by exception for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that network communications traffic is denied by default and allowed by exception at managed interfaces for the system.

4.1.16.3.4 SC-7[7] Prevent Split Tunneling for Remote Devices

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC prevents remote devices (e.g., laptops) from simultaneously establishing non-remote connections and communicating via some other connection to resources in external networks.

Provider Responsibilities:

OIS must:

- Prevent NRC-issued remote devices, from simultaneously establishing non-remote connections and communicating via some other connection to resources in external networks by disabling split tunneling on VPN client software.

System owners must:

- Ensure that the system prevents remote devices from simultaneously establishing non-remote connections and communicating via some other connection to resources in external networks for the system.

4.1.16.3.5 SC-7[8] Route Traffic To Authenticated Proxy Servers

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC routes internal communications traffic in accordance with CSO-STD-0020 and other NRC requirements through authenticated proxy servers at managed interfaces.

Provider Responsibilities:

CSO must:

- Define the types of internal communications traffic that must be routed through authenticated proxy servers to all external networks.

OIS must:

- Route internal communications traffic in accordance with CSO-STD-0020 and other NRC requirements through authenticated proxy servers at managed interfaces for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that internal communications traffic is routed in accordance with CSO-STD-0020 and other NRC requirements through authenticated proxy servers at managed interfaces for the system.

4.1.16.3.6 SC-7[18] Fail Secure

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC ensures the system fails securely in the event of an operational failure of a boundary protection device.

Provider Responsibilities:

OIS must:

- Ensure that NRC systems connected to NRC managed networks fail securely in the event of an operational failure of a boundary protection device.

System owners must:

- Ensure the system fails securely in the event of an operational failure of a boundary protection device.

4.1.16.3.7 SC-7[21] Isolation of Information System Components

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC employs boundary protection mechanisms to separate information system components in accordance with CSO-STD-0020.

Provider Responsibilities:

CSO must:

- Defiine the system components and the missions and/or business functions they support that require isolation.

OIS must:

- Employ boundary protection mechanisms to separate information system components for NRC systems connected to the NRC managed networks in accordance with CSO-STD-0020.

System owners must:

- Ensure boundary protection mechanisms to separate information system components is provided for the system in accordance with CSO-STD-0020 and other NRC requirements.

4.1.16.4 SC-10 Network Disconnect

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC terminates the network connection associated with a communications session in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Define the time period of inactivity that a system terminates a network session

OIS must:

- Terminate the network connection associated with a communications session in accordance with CSO-STD-0020 and other NRC requirements for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure the network connection associated with a communications session is terminated for the system in accordance with CSO-STD-0020 and other NRC requirements.

4.1.16.5 SC-17 Public Key Infrastructure Certificates

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC issues public key certificates in accordance with CSO-STD-2009.

Provider Responsibilities:

CSO must:

- Define certificate policies for issuing public key certificates.

OIS must:

- Issue public key certificates in accordance with CSO-STD-2009 for systems using NRC-provided network services.

System owners must:

- Ensure that are implemented in accordance with CSO-STD-2009 for systems that don't use public key certificates issued by OIS.

4.1.16.6 SC-18 Mobile Code

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Defines acceptable and unacceptable mobile code and mobile code technologies;
- Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- Authorizes, monitors, and controls the use of mobile code within the information system.

Provider Responsibilities:

CSO must:

- Provide policy and requirements for protection against malicious code and mobile code technologies.
- Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

OIS must:

- Define acceptable and unacceptable mobile code technologies.

System owners must:

- Define acceptable and unacceptable mobile code used within the information system.
- Monitor, and control the use of mobile code within the information system in accordance with CSO-STD-0020 and other NRC requirements.

4.1.16.7 SC-19 Voice Over Internet Protocol

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Establishes usage restrictions and requirements for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
- Authorizes, monitors, and controls the use of VoIP within the information system.

Provider Responsibilities:

CSO must:

- Establish usage restrictions and requirements for VoIP technologies.

System owners must:

- Authorize, monitor, and control the use of VoIP within the system in accordance with NRC requirements.

4.1.16.8 SC-20 Secure Name / Address Resolution Service (Authoritative Source)

This is a ***hybrid*** security control with responsibilities for the **OIS** and **system owners**.

Control Description:

The NRC:

- Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
- 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.

Provider Responsibilities:

OIS must:

- Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries for NRC systems connected to the NRC managed networks.
- Provide 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 for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that secure name/address resolution services are provided for the system.

4.1.16.9 SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

This is a ***hybrid*** security control with responsibilities for the **OIS** and **system owners**.

Control Description:

The NRC requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Provider Responsibilities:

OIS must:

- Provide secure name and address resolution services for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that secure name and address resolution services are provided for the system.

4.1.16.10 SC-22 Architecture and Provisioning for Name / Address Resolution Service

This is a ***hybrid*** security control with responsibilities for the **OIS** and **system owners**.

Control Description:

The NRC provides name/address resolution service for an organization that are fault-tolerant and implement internal/external role separation.

Provider Responsibilities:

OIS must**:**

- Provide name/address resolution service for NRC systems connected to the NRC managed networks that are fault-tolerant and implement internal/external role separation.

System owners must:

- Ensure that name and address resolution services are fault-tolerant and implement internal/external role separation for the system.

4.1.17 System and Information Integrity

Table 4.1-17 summarizes the common and hybrid security control responsibilities for the SI family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.1-17: SI Family Common and Hybrid Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
SI-1	System and Information Integrity Policy and Procedures	CSO, System Owners	Hybrid
SI-2	Flaw Remediation	CSO, System Owners	Hybrid
SI-2[1]	Central Management	System Owners	System Specific
SI-2[2]	Automated Flaw Remediation Status	System Owners	System Specific
SI-3	Malicious Code Protection	CSO, OIS, System Owners	Hybrid
SI-3[1]	Central Management	OIS, System Owners	Hybrid
SI-3[2]	Automatic Updates	OIS, System Owners	Hybrid
SI-4	Information System Monitoring	System Owners	System Specific
SI-4[2]	Automated Tools for Real-Time Analysis	System Owners	System Specific
SI-4[4]	Inbound and Outbound Communications Traffic	System Owners	System Specific
SI-4[5]	System-Generated Alerts	System Owners	System Specific
SI-5	Security Alerts, Advisories, and Directives	CSO, System Owners	Hybrid
SI-5[1]	Automated Alerts and Advisories	CSO	Common
SI-6	Security Function Verification	System Owners	System Specific
SI-7	Software, Firmware, and Information Integrity	System Owners	System Specific
SI-7[1]	Integrity Checks	System Owners	System Specific
SI-7[2]	Automated Notifications of Integrity Violations	System Owners	System Specific
SI-7[5]	Automated Response to Integrity Violations	System Owners	System Specific
SI-7[7]	Integration of Detection and Response	System Owners	System Specific
SI-7[14]	Binary or Machine Executable Code	System Owners	System Specific
SI-8	Spam Protection	OIS, System Owners	Hybrid
SI-8[1]	Central Management	OIS, System Owners	Hybrid
SI-8[2]	Automatic Updates	OIS, System Owners	Hybrid
SI-10	Information Input Validation	System Owners	System Specific
SI-11	Error Handling	System Owners	System Specific
SI-12	Information Handling and Retention	System Owners	System Specific
SI-16	Memory Protection	System Owners	System Specific

4.1.17.1 SI-1 System and Information Integrity Policy and Procedures

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Develops, documents, and disseminates to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements:
  - A system and information integrity policy that addresses purpose, scope, roles, responsibilities, organization–defined values, management commitment, coordination among NRC entities, and compliance; and
  - Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls;
- Reviews and updates the current:
  - System and information integrity policy in accordance with CSO-STD-0020 and other NRC requirements; and
  - System and information integrity procedures in accordance with CSO-STD-0020 and other NRC requirements.

Provider Responsibilities:

CSO must:

- Develop, document, review/update agency-wide system and information integrity policy and requirements as it applies to NRC systems and distribute to NRC users.

System owners must:

- Ensure that system-specific system and information integrity policy and procedures are developed, reviewed and maintained for the systems in accordance with NRC requirements.
- Ensure that system-specific system and information integrity procedures facilitate the implementation of system and information integrity policy.

4.1.17.2 SI-2 Flaw Remediation

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Identifies, reports, and corrects information system flaws;
- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

- Installs security-relevant software and firmware updates within in accordance with CSO-STD-0020 and other NRC requirements of the release of the updates; and
- Incorporates flaw remediation into the organizational configuration management process.

Provider Responsibilities:

CSO must:

- Define the time period for installing security-relevant software and firmware updates.

System owners must:

- Ensure that software and firmware updates are tested for effectiveness and potential side effects before installation;
- Install security-relevant software and firmware updates within in accordance with CSO-STD-0020 and other NRC requirements of the release of the updates; and
- Incorporate flaw remediation into the configuration management process.

4.1.17.3 SI-3 Malicious Code Protection

This is a ***hybrid*** security control with responsibilities for the **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
- Updates malicious code protection mechanisms whenever new releases are available in accordance with NRC configuration management policies and procedures;
- Configures malicious code protection mechanisms to:
  - Perform periodic scans of the information system 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
  - Ensure that response to malicious code detection is managed in accordance with CSO-STD-2108;
- Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Provider Responsibilities:

CSO must:

- Provide malicious code protection policy and requirements.

OIS must:

- Provide malicious code protection mechanisms for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that malicious code protection mechanisms are provided at information system entry and exit points to detect and eradicate malicious code;
- Ensure that malicious code protection mechanisms are updated whenever new releases are available in accordance with NRC configuration management policies and procedures;
- Ensure that malicious code protection mechanisms are configured in accordance with CSO-STD-2108; and
- Ensure that the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system is addressed.

4.1.17.3.1 SI-3[1] Central Management

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC centrally manages malicious code protection mechanisms.

Provider Responsibilities:

OIS must:

- Centrally manage malicious code protection mechanisms for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that malicious code protection mechanisms are centrally managed for the system.

4.1.17.3.2 SI-3[2] Automatic Updates

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC automatically updates malicious code protection mechanisms.

Provider Responsibilities:

OIS must:

- Automatically update malicious code protection mechanisms for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that malicious code protection mechanisms are automatically updated for the system.

4.1.17.4 SI-5 Security Alerts, Advisories, and Directives

This is a ***hybrid*** security control with responsibilities for the **CSO** and **system owners**.

Control Description:

The NRC:

- Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis in accordance with CSO-STD-0020 and other NRC requirements;
- Generates internal security alerts, advisories, and directives as deemed necessary;
- Disseminates security alerts and directives to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements; and
- Implements security directives (issued by Office of Management and Budget [OMB]) in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Provider Responsibilities:

CSO must:

- Receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis in accordance with CSO-STD-0020 and other NRC requirements;
- Generate internal security alerts, advisories, and directives via NRC email and Network Announcements as deemed appropriate;
- Disseminate security alerts and directives to NRC-defined personnel or roles in accordance with CSO-STD-0020 and other NRC requirements; and
- Notifies the issuing organization of the degree of noncompliance.

System Owners must:

- Implement security directives in accordance with established time frames issued by the issuing organization (e.g., US-CERT, OMB).

4.1.17.4.1 SI-5[1] Automated Alerts and Advisories

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC employs automated mechanisms to make security alert and advisory information available throughout the organization.

Provider Responsibilities:

CSO must:

- Employ automated mechanisms (e.g., NRC email and Network Announcements) to make security alert and advisory information available throughout the organization.

4.1.17.5 SI-8 Spam Protection

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC:

- Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
- Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Provider Responsibilities:

OIS must:

- Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages for NRC systems connected to the NRC managed networks.
- Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

System owners must:

- Ensure that spam protection at information system entry and exit points are employed to detect and take action on unsolicited messages.
- Ensure that spam protection mechanisms are updated for the system when new releases are available.

4.1.17.5.1 SI-8[1] Central Management

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC centrally manages spam protection mechanisms.

Provider Responsibilities:

OIS must:

- Centrally manage spam protection mechanisms for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that spam protection is centrally managed for the system.

4.1.17.5.2 SI-8[2] Automatic Updates

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC automatically updates spam protection mechanisms.

Provider Responsibilities:

OIS must:

- Automatically update spam protection mechanisms for NRC systems connected to the NRC managed networks.

System owners must:

- Ensure that spam protection is automatically updated for the system.

4.2 Program Management Controls

Office Directors and system owners have the overall responsibility for the security of NRC systems owned by NRC or operated on behalf of NRC by another agency or by a contractor. Because NRC systems support NRC operations and assets, system owners also have specific responsibilities for the successful implementation of the overall NRC information security program, specifically program management controls that are hybrid.

4.2.1 Program Management

Table 4.2-1 summarizes the common and hybrid security control responsibilities for the PM family of controls. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.2-1: PM Security Control Assignments

Control ID	Control Title	Provider(s)	Control Type
PM-1	Information Security Program Plan	CSO	Common
PM-2	Senior Information Security Officer	OEDO	Common
PM-3	Information Security Resources	OIS, Office Directors/ Regional Administrators, System Owners	Hybrid
PM-4	Plan of Action & Milestones Process	CSO	Common
PM-5	Information System Inventory	OIS, System Owners	Hybrid
PM-6	Information Security Measures of Performance	CSO, System Owners	Hybrid
PM-7	Enterprise Architecture	CSO, OIS	Common
PM-8	Critical Infrastructure Plan	CSO, OIS , NSIR, System Owners	Hybrid
PM-9	Risk Management Strategy	CSO	Common
PM-10	Security Authorization Process	CSO	Common
PM-11	Mission / Business Process Definition	CSO, OIS, Office Directors/Regional Administrators	Common
PM-12	Insider Threat Program	CSO, ADM, NSIR, OCHCO, Office of Chief Financial Officer (OCFO), Office of Genral Counsel (OGC), Office of Investigations (OI), Office of Inspector General (OIG), Office of International Programs (OIP), OIS	Common
PM-13	Information Security Workforce	CSO, OCHCO	Common
PM-14	Testing, Training, and Monitoring	CSO, OCHCO	Common

Control ID	Control Title	Provider(s)	Control Type
PM-15	Contacts with Security Groups and Associations	CSO	Common
PM-16	Threat Awareness Program	CSO, OIS	Common

4.2.1.1 PM-1 Information Security Program Plan

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC:

- Develops and disseminates an NRC-wide information security program plan that:
  - Provides an overview of the requirements for the security program and a description of the security program management controls and common security controls in place or planned for meeting those requirements;
  - Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
  - Reflects coordination among NRC entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
  - 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;
- Reviews the NRC-wide information security program plan in accordance with CSO-STD-0020 and NRC-defined MDs;
- Updates the plan to address NRC changes and problems identified during plan implementation or security control assessments; and
- Protects the information security program plan from unauthorized disclosure and modification.

Provider Responsibilities:

CSO must:

- Develop and disseminate an NRC-wide information security program plan that:
  - Provides an overview of the requirements for the security program and a description of the security program management controls and common security controls in place or planned for meeting those requirements;

- Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- Reflects coordination among NRC entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
- Ensures that NRC-wide information security program plan 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.

- Review the NRC-wide information security program plan in accordance with CSO-STD-0020 and NRC-defined MDs.
- Update the plan to address NRC changes and problems identified during plan implementation or security control assessments.
- Protect the information security program plan from unauthorized disclosure and modification.

4.2.1.2 PM-2 Senior Information Security Officer

This is a ***common*** security control with responsibilities for the **OEDO**.

Control Description:

The NRC appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an NRC-wide information security program.

Provider Responsibilities:

OEDO must:

- Appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an NRC-wide information security program.

4.2.1.3 PM-3 Information Security Resources

This is a ***hybrid*** security control with responsibilities for the **OIS**, **Office Directors and Regional Administrators**, and **system owners**.

Control Description:

The NRC:

- 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;
- Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and

- Ensures that information security resources are available for expenditure as planned.

Provider Responsibilities:

OIS must:

- Provide policy, guidance and oversight of the investment management process supporting the life cycle of every information technology (IT) project.
- Prioritize, validate and recommend (via the information technology board (ITB)) projects from across the agency for inclusion in the IT/Information management portfolio in accordance with IT governance and budget formulation processes. The ITB reviews agency IT submissions to ensure mission alignment, compliance with senior leadership guidance and that information security resources are included in all proposed investments.
- Prioritize, validate and strategically align (via the IT/Information management portfolio executive council [IPEC]) investments in this portfolio to support the agency mission.

Office Directors and Regional Administrators must**:**

- Endorse system owner allocation, budgeting and IT investment execution plans that support the agency mission. These plans must meet ITB specifications, include information security resource requirements, support the development of agency OMB Exhibit 53, Exhibit 500 products and support the agency mission.

System owners must:

- As part of the system development lifecycle create IT investment plans that support the agency mission.
- These plans must include information security resource requirements, meet ITB specifications, support the development of agency OMB Exhibit 53, Exhibit 500 products.
- IT investment plans must be endorsed by office directors/regional administrators.

4.2.1.4 PM-4 Plan of Action and Milestones Process

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC:

- Implements a process for ensuring that plans of action and milestones for the security program and associated NRC information systems:
  - Are developed and maintained;

  - Document the remedial information security actions to adequately respond to risk to NRC operations and assets, individuals, other organizations, and the Nation; and
  - Are reported in accordance with OMB FISMA reporting requirements;

- Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Provider Responsibilities:

CSO must:

- Implement a process for ensuring that plans of action and milestones for the security program and associated NRC information systems:
  - Are developed and maintained;
  - Document the remedial information security actions to adequately respond to risk to NRC operations and assets, individuals, other organizations, and the Nation; and
  - Are reported in accordance with OMB FISMA reporting requirements.
- Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

4.2.1.5 PM-5 Information System Inventory

This is a ***hybrid*** security control with responsibilities for the **OIS** and **system owners**.

Control Description:

The NRC develops and maintains an inventory of its information systems.

Provider Responsibilities:

OIS must:

- Develop and maintain the agency inventory for NRC information systems.

System owners must:

- Ensure that a current inventory for the system components is maintained, reviewed, and updated accordingly and provided to OIS.

4.2.1.6 PM-6 Information Security Measures of Performance

This is a ***hybrid*** security control with responsibilities for **CSO** and **system owners**.

Control Description:

The NRC develops, monitors, and reports on the results of information security measures of performance.

Provider Responsibilities:

CSO must:

- Develop, monitor, and report on the results of information security measures of performance to measure the effectiveness or efficiency of the NRC information security program and the security controls employed in support of the program.

System owners must:

- Provide results from security measures of performance activities to CSO.

4.2.1.7 PM-7 Enterprise Architecture

This is a ***common*** security control with responsibilities for the **CSO** and **OIS** .

Control Description:

The NRC develops an enterprise architecture (EA) with consideration for information security and the resulting risk to NRC operations, NRC assets, individuals, other organizations, and the Nation.

Provider Responsibilities:

CSO must:

- Provide policy and requirements for the NRC's EA to ensure that security requirements are integrated into the EA consistent with organizational risk management and information security strategies.

OIS must:

- Provide policy, guidelines, and processes.
- Implement the NRC's EA program, which includes documenting NRC's EA models, maintaining the EA Transition Plan and EA Program Plan, supporting the Baseline and Target EA models, aligning the NRC's EA with the Federal EA (FEA).
- Ensure EA compliance with OMB and other Federal requirements. The Information Technology/Information Management (IT/IM) Architecture Council review and approval process is required to add new technology to the NRC environment. This ensures information security requirements and associated security controls are incorporated into the Technical Reference Model (TRM) of the EA.

4.2.1.8 PM-8 Critical Infrastructure Plan

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, **NSIR**, and **system owners**.

Control Description:

The NRC addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Provider Responsibilities:

CSO must:

- Identify cybersecurity requirements that must be incorporated into the COOP.

OIS must:

- Provide capabilities to quickly transfer NRC managed networks based systems in accordance with the NRC Continuity of Operations Plan (COOP).

NSIR must:

- Ensure cybersecurity requirements are incorporated appropriately into the COOP.

System owners must:

- Ensure systems designated as COOP systems can readily transfer to the alternate site identified in the COOP for the system.

4.2.1.9 PM-9 Risk Management Strategy

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC:

- 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 systems;
- Implements the risk management strategy consistently across the agency; and
- Reviews and updates the risk management strategy within the NRC-defined frequency or as required, to address NRC changes.

Provider Responsibilities:

CSO must:

- Provide 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 systems.
- Implement the risk management strategy consistently across the agency.
- Review and update the risk management strategy in accordance with CSO-STD-0020 and other NRC requirements or as required, to address NRC changes.

4.2.1.10 PM-10 Security Authorization Process

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC:

- Manages (i.e., documents, tracks, and reports) the security state of NRC information systems and the environments in which those systems operate through security authorization processes;
- Designates individuals to fulfill specific roles and responsibilities within the NRC risk management process; and
- Fully integrates the security authorization processes into an NRC-wide risk management program.

Provider Responsibilities:

CSO must:

- Manage (i.e., documents, tracks, and reports) the security state of NRC information systems and the environments in which those systems operate through security authorization processes.
- Designate individuals to fulfill specific roles and responsibilities within the NRC risk management process.
- Fully integrate the security authorization processes into an NRC-wide risk management program.

4.2.1.11 PM-11 Mission / Business Process Definition

This is a ***common*** security control with responsibilities for the **CSO**, **OIS** , and **Office Directors and Regional Administrators**.

Control Description:

The NRC:

- Defines mission/business processes with consideration for information security and the resulting risk to NRC operations, NRC assets, individuals, other organizations, and the Nation; and
- Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

NRC Supplemental Information:

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 systems 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.

Provider Responsibilities:

CSO must:

- Provide policy and requirements for conducting the security categorization, which is completed as part of the Business Case documents in order to determine the impact level of the IT system processing the information for the defined business processes. Information types are mapped to the Business Area, Line of Business, and Sub-Function from the FEA Business Reference Model listed in the Business Case and associated impact levels are assessed in accordance with NIST SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories," and FIPS Publication (PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems."
- Review and approve the Security Categorization document in order for the project to proceed to the next step in the Risk Management Framework.

OIS must:

- Provide policy, guidance, and coordination for the CPIC process, a component of the Project Management Methodology (PMM) to ensure definition of mission/business processes with consideration for information security and resulting risk.
- Identify this information in Business Case documents, which must be reviewed and assessed by the Information Technology Business Council (ITBC) and approved by the

CIO or OIS depending on the tier level in order to receive approval to proceed to the next phase of the CPIC and PMM Processes.

Office Directors and Regional Administrators must:

- Define the mission/business needs and supporting processes for determining the level of information protection required and establish the level of adverse impact that could result if a compromise of information occurs.

4.2.1.12 PM-12 Insider Threat Program

This is a ***common*** security control with responsibilities for the **NSIR**.

Control Description:

The NRC implements an insider threat program that includes a cross-discipline insider threat incident handling team.

Provider Responsibilities:

NSIR must:

- Administer the NRC's insider threat program.

Note to ISSO Forum: The composition and responsibilities of the NRC insider threat program is still being finalized. This will be updated (if necessary) once the composition and responsibilities are finalized.

4.2.1.13 PM-13 Information Security Workforce

This is a ***common*** security control with responsibilities for the **CSO** and **OCHCO**.

Control Description:

The NRC establishes an information security workforce development and improvement program.

Provider Responsibilities:

CSO must:

- Define the knowledge and skill levels needed to perform information security duties and tasks and provides guidance to OCHCO.
- Ensure that training courses include the correct information for the roles identified.

OCHCO must:

- Establish a workforce development and improvement program to fill information security-related NRC positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs.

4.2.1.14 PM-14 Testing, Training, and Monitoring

This is a ***common*** security control with responsibilities for the **CSO** and **OCHCO**.

Control Description:

The NRC:

- Implements a process for ensuring that agency plans for conducting security testing, training, and monitoring activities associated with NRC information systems:
  - Are developed and maintained; and
  - Continue to be executed in a timely manner;
- Reviews testing, training, and monitoring plans for consistency with the NRC risk management strategy and agency-wide priorities for risk response actions.

Provider Responsibilities:

CSO must:

- Provide policy, requirements, coordination, and oversight for the security testing, training, and monitoring activities conducted for NRC systems.

OCHCO must:

- Implement a process for ensuring that security testing and training are developed, maintained and monitored in a timely manner and monitoring program.
- Review testing, training, and monitoring plans for consistency with the NRC risk management strategy and agency-wide priorities for risk response actions.

4.2.1.15 PM-15 Contacts with Security Groups and Associations

This is a ***common*** security control with responsibilities for the **CSO**.

Control Description:

The NRC establishes and institutionalizes contact with selected groups and associations within the security community:

- To facilitate ongoing security education and training for NRC personnel;
- To maintain currency with recommended security practices, techniques, and technologies; and
- To share current security-related information including threats, vulnerabilities, and incidents.

Provider Responsibilities:

CSO must:

- Maintain ongoing contact with security groups, forums, and/or peer groups of security professionals in similar organizations to provide ongoing security education and training, remain current with recommended security practices, and to share current security-related information including threats, vulnerabilities, and incidents.

4.2.1.16 PM-16 Threat Awareness Program

This is a ***common*** security control with responsibilities for the **CSO** and **OIS**.

Control Description:

The NRC implements a threat awareness program that includes a cross-agency information-sharing capability.

Provider Responsibilities:

CSO must:

- Maintain ongoing contact with security groups, forums and/or peer groups of security professionals in similar organizations to share mitigation tactics, techniques and procedures that have been found effective against the sophistication of adversaries, especially the advanced persistent threat (APT).

OIS must:

- Disseminate threat awareness information to system owners and ISSOs as it becomes available.

4.3 Privacy Controls

Table 4.3-1 summarizes the common and hybrid security control responsibilities for the Privacy Control family. Detailed sections that follow describe the provider responsibilities for implementing common and hybrid security controls.

Table 4.3-1: **Privacy Control Family Common and Hybrid Security Control Assignments**

Control ID	Control Title	Provider(s)	Control Type
AP-1	Authority to Collect	OIS, System Owners	Hybrid
AP-2	Purpose Specification	OIS, System Owners	Hybrid
AR-1	Governance and Privacy Program	OEDO, CSO, OIS	Common
AR-2	Privacy Impact and Risk Assessment	OIS, System Owners	Hybrid
AR-3	Privacy Requirements for Contractors and Service Providers	OIS, ADM, System Owners	Hybrid
AR-4	Privacy Monitoring and Auditing	CSO, OIS, OIG, System Owners	Hybrid
AR-5	Privacy Awareness and Training	CSO, OIS, OCHCO	Common
AR-6	Privacy Reporting	CSO, OIS	Common
AR-7	Privacy-Enhanced System Design and Development	System Owners	System Specific
AR-8	Accounting of Disclosures	OIS, System Owners	Hybrid
DI-1	Data Quality	System Owners	System Specific
DI-1[1]	Validate Personally Identifiable Information (PII)	System Owners	System Specific
DI-1[2]	Re-Validate PII	System Owners	System Specific
DI-2	Data Integrity and Data Integrity Board	OIS	Common
DI-2[1]	Publish Agreements on Website	OIS	Common
DM-1	Minimization of Personally Identifiable Information	CSO, OIS, System Owners	Hybrid
DM-1[1]	Locate / Remove / Redact / Anonymize PII	System Owners	System Specific
DM-2	Data Retention and Disposal	CSO, OIS, System Owners	Hybrid
DM-2[1]	System Configuration	System Owners	System Specific
DM-3	Minimization of PII Used in Testing, Training, and Research	System Owners	System Specific
DM-3[1]	Risk Minimization Techniques	System Owners	System Specific
IP-1	Consent	System Owners	System Specific
IP-1[1]	Mechanisms Supporting Itemized or Tiered Consent	System Owners	System Specific
IP-2	Individual Access	OIS, System Owners	Hybrid
IP-3	Redress	System Owners	System Specific

Control ID	Control Title	Provider(s)	Control Type
IP-4	Complaint Management	OIS, System Owners	Hybrid
IP-4[1]	Response Times	CSO, OIS, System Owners	Hybrid
SE-1	Inventory of Personally Identifiable Information	CSO, OIS, System Owners	Hybrid
SE-2	Privacy Incident Response	CSO, ADM, OIS	Common
TR-1	Privacy Notice	OIS, System Owners	Hybrid
TR-1[1]	Real-Time or Layered Notice	System Owners	System Specific
TR-2	System of Records Notices and Privacy Act Statements	OIS, System Owners	Hybrid
TR-2[1]	Public Website Publication	ADM	Common
TR-3	Dissemination of Privacy Program Information	OIS	Common
UL-1	Internal Use	OCHCO, OIS, System Owners	Hybrid
UL-2	Information Sharing with Third Parties	OIS, System Owners	Hybrid

4.3.1 Authority and Purpose

4.3.1.1 AP-1 Authority to Collect

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

Provider Responsibilities:

OIS must:

- Establish and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.
- Determine whether the contemplated collection of PII is legally authorized.

System owners must:

- Submit a Privacy Threshold Analysis (PTA) to determine if a Privacy Impact Assessment (PIA) is necessary; or
- Develop and submit a PIA for the information system to obtain permission to collect, use, maintain, and share PII in support of a specific system need.

4.3.1.2 AP-2 Purpose Specification

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

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

Provider Responsibilities:

OIS must:

- Establish and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

System owners must:

- Submit a PTA to determine if a PIA is necessary; or
- Develop and submit a PIA for the information system that describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.

4.3.2 Accountability, Audit, and Risk Management

4.3.2.1 AR-1 Governance and Privacy Program

This is a ***common*** security control with responsibilities for **OEDO**, **CSO**, and **OIS**.

Control Description:

The NRC:

- 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 PII by programs and information systems;
- Monitors federal privacy laws and policy for changes that affect the privacy program;

- Allocates sufficient resources to implement and operate the organization-wide privacy program in accordance with MD 3.2, CSO-STD-0020, and other NRC requirements;
- Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
- Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
- Updates privacy plan, policies, and procedures in accordance with MD 3.2, CSO-STD-0020, and other NRC requirements.

Provider Responsibilities:

OEDO must:

- Appoint a SAOP/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 PII by programs and information systems.

CSO must:

- Define the type of resources to implement and operate the NRC-wide privacy program.
- Define the timeframe for updating privacy plan, policies and procedures.

OIS must:

- Monitor federal privacy laws and policy for changes that affect the privacy program.
- Allocate sufficient resources to implement and operate the organization-wide privacy program in accordance with MD 3.2, CSO-STD-0020, and other NRC requirements.
- Develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures.
- Develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.
- Update privacy plans, policies, and procedures in accordance with MD 3.2, CSO-STD-0020, and other NRC requirements.

4.3.2.2 AR-2 Privacy Impact and Risk Assessment

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC:

- 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 PII; and
- Conducts PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Provider Responsibilities:

OIS must:

- Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII in accordance with MD 3.2, Privacy Act.
- Review and approve the PIA for the applicability of the Privacy Act, Paperwork Reduction Act information collection requirements, and Federal Records Act records management requirements.
- Add the PIA to the Agencywide Documents Access and Management System (ADAMS) and insert the assigned accession number (e.g., ML10001A001) into the upper left corner of the first page.
- Email the finalized PIA review results to:

    1. Sponsoring office (program manager and system owner)
    2. Director, Solutions Development Division (SDD)
    3. SITSO

System owners must:

- Submit a PTA to determine if a PIA is necessary. If so, conduct a PIA for the information system to identify privacy risks and identify methods to mitigate those risks in accordance with applicable law, OMB policy, MD 3.2, or any existing organizational policies and procedures.

4.3.2.3 AR-3 Privacy Requirements for Contractors and Service Providers

This is a ***common*** security control with responsibilities for **OIS**, **ADM**, and **system owners**.

Control Description:

The NRC:

- Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and
- Includes privacy requirements in contracts and other acquisition-related documents.

Provider Responsibilities:

OIS must:

- Establish privacy roles, responsibilities, and access requirements for contractors and service providers.

ADM must:

- Include privacy requirements in contracts and other acquisition-related documents for contractors and service providers.

System owners must:

- Ensure that privacy roles, responsibilities, and access requirements for contractors and service providers are in accordance with NRC requirements.

4.3.2.4 AR-4 Privacy Monitoring and Auditing

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, **OIG**, and **system owners**.

Control Description:

The NRC monitors and audits privacy controls and internal privacy policy in accordance with CSO-STD-0020 and other NRC requirements to ensure effective implementation.

Provider Responsibilities:

CSO must:

- Define the frequency for monitoring and auditing privacy controls and internal privacy policy.

OIS must:

- Monitor for changes to applicable privacy laws, regulations, and policies and communicate those changes to system owners.

OIG must:

- Conduct audits of the NRC privacy program to ensure compliance with applicable privacy laws, regulations, and policies.

System owners must:

- Conduct assessments in accordance with CSO-STD-0020 and other NRC requirements to ensure that the management, operational and technical controls are implemented effectively to protect PII.
- Monitor the system to ensure that access to PII is based on need-to-know and used only for the legally authorized purposes identified in the public notice.

4.3.2.5 AR-5 Privacy Awareness and Training

This is a ***common*** security control with responsibilities for **CSO**, **OIS**, and **OCHCO**.

Control Description:

The NRC:

- Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
- Administers basic and role-based privacy training at least annually; and
- Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually.

Provider Responsibilities:

CSO must:

- Define the frequency for administerinig basic privacy training and targeted, role-based privacy training.

OIS must:

- Assist OCHCO in training development to ensure comprehensiveness and accuracy of information.

OCHCO must:

- Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.
- Administer basic and role-based privacy training in accordance with CSO-STD-0020 and other NRC requirements.

- Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements in accordance with CSO-STD-0020 and other NRC requirements.
- Defiine the frequency and method for acceptance of responsibilities for privacy requirements.

4.3.2.6 AR-6 Privacy Reporting

This is a ***common*** security control with responsibilities for **CSO** and **OIS**.

Control Description:

The NRC develops, disseminates, and updates reports to the 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.

Provider Responsibilities:

CSO must:

- Provide OIS privacy reports to OMB/DHS through CyberScope.

OIS must:

- Develop, disseminate, and update reports to the 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.
- Provide privacy reports to CSO to meet FISMA reporting requirements.

4.3.2.7 AR-8 Accounting of Disclosures

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC:

- Keeps an accurate accounting of disclosures of information held in each system of records under its control, including, date, nature, and purpose of each disclosure of a record and name and address of the person or agency to which the disclosure was made;
- Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
- Makes the accounting of disclosures available to the person named in the record upon request.

Provider Responsibilities:

OIS must:

- Periodically consult with system owners to ensure that the required accountings of disclosures of records are being properly maintained consistent with the dictates of the Privacy Act.

System owners must:

- Keep an accurate accounting of disclosures of information in the system of records under its control; including, date, nature, and purpose of each disclosure of a record; and name and address of the person or agency to which the disclosure was made.
- Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer.
- Make the accounting of disclosures available to the person named in the record upon request.

4.3.3 Data Quality and Integrity

4.3.3.1 DI-2 Data Integrity and Data Integrity Board

This is a ***common*** security control with responsibilities for **OIS**.

Control Description:

The NRC:

- Documents processes to ensure the integrity of PII through existing security controls; and
- Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Provider Responsibilities:

OIS must:

- Establish a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

4.3.3.1.1 DI-2[1] Publish Agreements on Website

This is a ***common*** security control with responsibilities for **OIS**.

The NRC:

- Publishes Computer Matching Agreements on its public website.

Provider Responsibilities:

OIS must:

- Publish Computer Matching Agreements on the NRC public website.

4.3.4 Data Minimization and Retention

4.3.4.1 DM-1 Minimization of Personally Identifiable Information

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
- 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
- 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.

Provider Responsibilities:

CSO must:

- Define the frequency for reviewing PII holdings.

OIS must:

- Establish and implement a privacy risk management process that identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection.
- Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings in accordance with CSO-STD-0020 and other NRC requirements 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.

System owners must:

- Limit 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.
- Review PII holdings in accordance with CSO-STD-0020 and other NRC requirements to ensure that only PII identified in the notice is collected and retained, and continues to be necessary to accomplish the legally authorized purpose.

4.3.4.2 DM-2 Data Retention and Disposal

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Retains each collection of PII in accordance with CSO-STD-0020 and other NRC requirements to fulfill the purpose(s) identified in the notice or as required by law;
- Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
- Uses NRC-defined techniques in accordance with CSO-STD-2004 to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Provider Responsibilities:

CSO must:

- Defiine the time period to retain each collecton of PII to fulfill the purpose identified in the System of Records Notice (SORN).
- Defiine the method of secure deletion or destruction of PII.

OIS must:

- Review system PIA to determine retention of PII and indicate to system owners what the retention schedule should be in accordance with NARA.

System owners must:

- Retain each collection of PII in accordance with CSO-STD-0020 and other NRC requirements to fulfill the purpose(s) identified in the notice or as required by law;
- Ensure retention schedule is documented in the PIA.
- Dispose of PII in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

- Use NRC-defined techniques in accordance with CSO-STD-2004 to ensure secure deletion or destruction of PII (including originals, copies, and archived records.

4.3.5 Individual Participation and Redress

4.3.5.1 IP-2 Individual Access

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC:

- Provides individuals the ability to have access to their PII maintained in its system(s) of records;
- Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
- Publishes access procedures in SORNs; and
- Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Provider Responsibilities:

OIS must:

- Provide the content of Privacy Act regulations and record request processing, in consultation with legal counsel.
- Publish access procedures in SORNs.

System owners must:

- Provide individuals the ability to have access to their PII maintained in its system(s) of records.
- Adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.
- Notify OIS of any PII access changes that need to be incorporated into the SORN.

4.3.5.2 IP-4 Complaint Management

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC:

- Provides complaint mechanisms that are readily accessible by the public, including all information necessary for successfully filing complaints (including contact information for the SAOP/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; and
- Implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Provider Responsibilities:

OIS must:

- Provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the SAOP/CPO or other official designated to receive complaints), and are easy to use.
- Include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.
- Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

System owners must:

- Implement a process for receiving, tracking and responding to complaints, concerns, or questions from individuals about the system's privacy practices.

4.3.5.2.1 IP-4 [1] Response Times

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC responds to complaints, concerns, or questions from individuals within 5 business days.

Provider Responsibilities:

CSO must:

- Define the time period for responding to complaints, concerns, or questions.

OIS must:

- Respond to complaints, concerns, or questions from individuals in accordance with CSO-STD-0020 and other NRC requirements.

System owners must:

- Respond to system complaints, concerns, or questions from individuals in accordance with CSO-STD-0020 and other NRC requirements.

4.3.6 Security

4.3.6.1 SE-1 Inventory of Personally Identifiable Information

This is a ***hybrid*** security control with responsibilities for **CSO**, **OIS**, and **system owners**.

Control Description:

The NRC:

- Establishes, maintains, and updates an inventory in accordance with CSO-STD-0020 and other NRC requirements that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and
- Provides each update of the PII inventory to the CIO or or information security official in accordance with CSO-STD-0020 and other NRC requirements to support the establishment of information security requirements for all new or modified information systems containing PII.

Provider Responsibilities:

CSO must:

- Define the frequency for maintaining and updating an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII to support the establishment of information security requirements.

OIS must:

- Establish, maintain, and update an inventory in accordance with CSO-STD-0020 and other NRC requirements that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.
- Provide each update of the PII inventory to the CIO or information security official in accordance with CSO-STD-0020 and other NRC requirements to support the establishment of information security requirements for all new or modified information systems containing PII.

System owners must:

- Ensure that a current inventory for the system components that contain PII is maintained, reviewed, and updated accordingly and provided to OIS in accordance with CSO-STD-0020 and other NRC requirements.

4.3.6.2 SE-2 Privacy Incident Response

This is a ***common*** security control with responsibilities for **CSO, ADM**, and **OIS**.

Control Description:

The NRC:

- Develops and implements a Privacy Incident Response Plan; and
- Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Provider Responsibilities:

CSO must:

- Develop and implement a Privacy Incident Response Plan that involves breaches of PII in electronic form in accordance with the organizational Privacy Incident Response Plan.

ADM must:

- Develop and implement a Privacy Incident Response Plan that involves breaches of PII in physical form in accordance with the organizational Privacy Incident Response Plan.

OIS must:

- Develop and implements a Privacy Incident Response Plan.
- Provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

4.3.7 Transparency

4.3.7.1 TR-1 Privacy Notice

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC:

- 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 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;
- 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
- 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.

Provider Responsibilities:

OIS must:

- Communicate changes in PII practice or policy as it relates to the content of privacy notices.

System owners must:

- Provide an effective privacy notice to individuals regarding its collection, use, sharing, safeguarding, maintenance, and disposal of PII.
- Provide an effective privacy notice to individuals describing the authority for collecting PII, how the system uses PII, the choices individuals may have regarding how the system uses PII and the ability to access and have PII amended or corrected if necessary.
- Provide an effective privacy notice to individuals describing whether PII with be shared with external entities, the categories of those entities, and the purposes for such sharing.
- Provide an effective privacy notice to individuals describing whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent.
- Provide an effective privacy notice to individuals describing how individuals may obtain access to PII and how the PII will be protected.

4.3.7.2 TR-2 System of Records Notices and Privacy Act Statements

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC:

- Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII;
- Keeps SORNs current; and
- 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.

Provider Responsibilities:

OIS must:

- Publish SORNs in the Federal Register, subject to required oversight processes, for systems containing PII;
- Keep SORNs current; and
- Include 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.

System owners must:

- Notify OIS of any PII changes that need to be incorporated into the SORN.

4.3.7.2.1 TR-2[1] Public Website Publication

This is a ***common*** security control with responsibilities for **ADM**.

Control Description:

The NRC publishes SORNs on its public website.

Provider Responsibilities:

ADM must:

- Publish SORNs on its public website.

4.3.7.3 TR-3 Dissemination of Privacy Program Information

This is a ***common*** security control with responsibilities for **OIS**.

Control Description:

The NRC:

- Ensures that the public has access to information about its privacy activities and is able to communicate with its SAOP/CPO; and
- Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Provider Responsibilities:

OIS must:

- Ensure that the public has access to information about its privacy activities and is able to communicate with its SAOP/CPO; and
- Ensure that its privacy practices are publicly available through organizational websites or otherwise.

4.3.8 Use Limitation

4.3.8.1 UL-1 Internal Use

This is a ***hybrid*** security control with responsibilities for **OCHCO**, **OIS**, and **system owners**.

Control Description:

The NRC uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Provider Responsibilities:

OCHCO must:

- Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

OIS must:

- Provide guidance from the SAOP/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.
- Assist OCHCO in training development.

System owners must:

- 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.

- Monitor and audit use of PII within the system.
- Ensure system personnel are trained on the authorized uses of PII.

4.3.8.2 UL-2 Information Sharing with Third Parties

This is a ***hybrid*** security control with responsibilities for **OIS** and **system owners**.

Control Description:

The NRC:

- Shares 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;
- 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;
- 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
- 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.

Provider Responsibilities:

OIS must:

- 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).

System owners must:

- Monitor, audit, and train staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

APPENDIX A. ACRONYMS

AC	Access Control
AD	Active Directory
ADAMS	Agencywide Documents Access and Management System
ADM	Office of Administration
AP	Authority and Purpose
APT	Advanced Persistent Threat
AR	Accountability, Audit, and Risk Management
AT	Awareness and Training
ATO	Authority to Operate
AU	Audit and Accountability
CA	Security Assessment and Authorization
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
CP	Contingency Planning
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
CSAAR	Cyber, Situational, Awareness, Analysis, and Response
CSC	Computer Support Center
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Office
DAA	Designated Approving Authority
DHS	Department of Homeland Security
DI	Data Quality and Integrity
DM	Data Minimization and Retention
DoS	Denial of Service
EA	Enterprise Architecture
ESSO	Enterprise Single Sign-On
FBCA	Federal Bridge Certification Authority
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management

FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IP	Individual Participation and Redress
IPEC	Information Technology/Information Management Portfolio Executive Council
IR	Incident Response
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer
IT	Information Technology
ITBC	Information Technology Business Council
IT/IM	Information Technology/Information Management
LAN	Locan Area Network
MA	Maintenance
MD	Management Directive
MOU	Memorandum of Understanding
MP	Media Protection
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSIR	Office of Nuclear Security and Incident Response
OCFO	Office of Chief Financial Officer
OCHCO	Office of the Chief Human Capital Officer
OEDO	Office of the Executive Director of Operations
OGC	Office of General Counsel
OI	Office of Investigations
OIG	Office of Inspector General
OIP	Office of International Programs
OIS	Office of Information Services
OMB	Office of Management and Budget
PACS	Physical Access Control System
PE	Physical and Environmental Protection
PCT	Policy, Compliance, and Training

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning
PM	Program Management
PMM	Project Management Methodology
PROS	Process
PS	Personnel Security
PTA	Privacy Threshold Analysis
PUB	Publication
RA	Risk Assessment
SA	System and Services Acquisition
SAOP	Senior Agency Official for Privacy
SC	System and Communications Protection
SE	Security
SDD	Solutions Development Division
SGI	Safeguards Information
SI	System and Information Integrity
SITSO	Senior Information Technology Security Officer
SLA	Service Level Agreement
SORN	System of Records Notice
SP	Special Publication
STD	Standard
SUNSI	Sensitive Unclassified Non-Safeguards Information
TR	Transparency
TRM	Technical Reference Model
UL	Use Limitation
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX B. DEFINITIONS

Common Security Control	A security control that is implemented at the organization-level and fulfilled for all NRC systems regardless of location. Because common security controls protect multiple organizational systems of differing impact levels, the controls are implemented with regard to the highest impact level among the systems.
Common Security Control Provider	A common security control provider is an office director, regional administrator, or OIS division director with overall responsibility for the development, implementation, assessment, and monitoring of a set of common security controls. Common security control providers, as the system owners for these systems, are accountable for the security risk associated with operating his/her system/common security controls. The common security control provider is an agency official who has inherent U.S. Government authority and must be a Government employee.
Hybrid Security Control	A security control that is implemented for an NRC system in part as a common security control (or inherited by another system) and in part as a system-specific security control.
Non-NRC Facility Owners	An individual, partnership, or corporation that owns and manages a facility that contains NRC data and assets.
NRC Requirements	Refers to NRC MDs, standards, processes, procedures, checklists, and guidance applicable to the security controls addressed in this standard.
Security Control Inheritance	A situation in which a system receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system.
System Owners	A system owner is an office director, regional administrator, or OIS division director that has overall responsibility for the security of NRC systems owned by his or her organization or operated on behalf of his or her organization by another agency or by a contractor. The system owner is an agency official who has inherent U.S. Government authority and must be a Government employee.
System-Specific Security Control	A security control for an NRC system that has not been designated as a common security control or

the portion of a hybrid security control that is to be implemented within a system. System-specific security controls are the primary responsibility of system owners.

CSO-STD-0021 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
29-Jul-15	1.0	Initial Release	ISSO forum and CSO web page	Upon request