Nuclear Regulatory Commission
Computer Security Office
Computer Security Process

Office Instruction:	CSO-PROS-2102
Office Instruction Title:	System Cybersecurity Assessment Process
Revision Number:	1.0
Issue Date:	July 24, 2015
Effective Date:	August 1, 2015
Primary Contacts:	Kathy Lyons Burke, SITSO
Responsible Organization:	CSO/PCT
Summary of Changes:	CSO-PROS-2102, "System Cybersecurity Assessment Process," provides the process that must be used in order to effectively conduct system cybersecurity assessments to support authorization decisions for systems storing or processing NRC information up to, and including, the Safeguards Information (SGI) level.
Training:	As requested
ADAMS Accession No.:	ML13338A366

Concurrences			
Primary Office Owner	Policy, Compliance, and Training		
Responsible SITSO	Kathy Lyons Burke		Date of Concurrence
Directors	CSO	Tom Rich	27-May-15
	PCT	Kathy Lyons Burke	27-May-15
	CSA	Thorne Graham (Charles Watkins for)	27-May-15

Concurrence Meeting Conducted on 27-May-15			
Attendees:	Tom Rich	Jon Feibus	Kathy Lyons-Burke
	Charles Watkins		

Table of Contents

Computer Security Process
CSO-PROS-2102
System Cybersecurity Assessment Process

1 PURPOSE

CSO-PROS-2102, “Nuclear Regulatory Commission (NRC) System Cybersecurity Assessment Process," provides the NRC approved process for conducting system cybersecurity assessments (SCAs) of systems that store, transmit, receive, or process NRC information up to, and including, the Safeguards Information (SGI) level. CSO-PROS-2102 can be used to perform an assessment of an entire system, a subsystem, or a well-defined part of a system. The results of the SCA-are documented in a SCA-report and provide an indication of the security state of the system, subsystem, or system component at the time of the assessment. SCAs are conducted to support system authorization decisions, including authorization of changes, by the NRC Designated Approving Authority (DAA) as well as to provide NRC officials with the state of cyber risk associated with a system, subsystem, or system component at any point in time.

The information in this document is intended to be used by system owners, Information System Security Officers (ISSOs), system administrators, assessment project managers, and assessors.

This process does not apply to the independent assessment of Federal Risk and Authorization Management Program (FedRAMP) certified cloud services from external providers; organizations must consult FedRAMP-when acquiring cloud services. FedRAMP-addresses required security controls and independent assessments for a variety of cloud services. Additional information is available at http://www.fedramp.gov.

2 GENERAL REQUIREMENTS

A critical aspect of the system security monitoring and authorization processes is an assessment of a system’s compliance with defined cybersecurity requirements. This is accomplished by testing the correctness and effectiveness of the cybersecurity controls implemented to meet the requirements. SCAs are conducted to determine the extent to which cybersecurity controls are implemented correctly, operating as intended, and producing the desired results.

The assessment results (documented in a SCA-report) provide insight into the current security state of a system. The DAA uses the SCA-report together with other relevant documents to determine the level of risk the system poses to NRC and makes authorization and monitoring decisions for the system.

2.1 Definitions

Activities An assessment object that includes specific protection related pursuits or actions supporting a system that involve people (e.g., conducting system backup operations, monitoring network traffic).

As-Built State The existing state of the system and system components at the time of the assessment. A system's configuration baseline should reflect the as built state of the system.

Assessment Boundary All components of a system identified as within scope for a particular assessment effort. For example, if the scope of a SCA-is defined as system components located at NRC headquarters buildings, regional components would be outside of the assessment boundary. These components would not be assessed and would not be selected in the SCA-plan for vulnerability scans and configuration checks. Hardware components within the assessment boundary are candidates for selection in the SCA-plan.

Assessment Finding The result of an assessor executing a determination statement within an assessment objective. Assessment findings include: Satisfied, Other than Satisfied, Provided at Agency Level, Provided by <XYZ System>, Risk-based Decision, and Not Applicable.

Assessment Method One of three types of actions (i.e., Interview, examine, test) taken by assessor(s) in obtaining evidence during an assessment.

Assessment Object The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.

Assessment Objective A set of determination statements that express the desired outcome for the assessment of a security control or control enhancement.

Assessment Procedure A set of assessment objectives and an associated set of assessment methods and assessment objects.

Assessment Project Manager The individual responsible for developing and distributing the project plan for the assessment, monitoring to ensure actions occur in accordance with the plan, and revising the plan if necessary during the course of the assessment. The assessment project manager serves as the primary contact for issues that may impact or delay key assessment activities.

Assessment Result The outcome of the assessment of the effectiveness of a security control as determined by an independent assessor, including all findings for specific assessment objectives, detailed notes concerning the findings, the overall security control status, and a detailed note concerning the status.

Assessor The individual(s) conducting security control testing, vulnerability scans, and configuration checks.

Assurance Requirement Requirements that establish a basis for confidence that a set of intended security controls in a system are effective in their application.

Authorization All components of a system to be authorized or already authorized by

Boundary the DAA.

Authorization Package A package of documents submitted to the DAA for the purpose of requesting an authorization decision. SCA-package deliverables are included as part of the authorization package.

Common Control A security control that is implemented at the organization level and fulfilled for all NRC systems regardless of location. Because common controls protect multiple organizational systems of differing impact levels, the controls are implemented with regard to the highest impact level among the systems. Common control providers are responsible for the development, implementation, assessment, and monitoring of common controls and are held accountable for the security risk associated with operating the common controls.

Common Control Provider An organizational official responsible for the development, implementation, assessment, and monitoring of common controls, and for the residual risk remaining after implementation of the control.

Computer Security Office (CSO) Representative The individual representing CSO and providing oversight throughout the SCA-effort to ensure that the effort is conducted per current NRC SCA-requirements. The CSO representative serves as the primary contact for NRC policy, guidance, direction, and resources throughout the course of the SCA.

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

Configuration Check A manual or automated comparison of a system component's current configuration against the required configuration, based on an NRC approved security configuration standard.

Coverage An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.

Depth An attribute associated with an assessment method (Interview, examine, or test) that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive.

Determination Statement A statement that expresses a desired outcome for the assessment of a security control or control enhancement. See Assessment Objective.

Examine A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.

FICAM-Approved Credentials Third party credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third party credentials meet or exceed the set of minimum federal government wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.

FICAM-Approved System Components Information technology products and software libraries that have been approved by the FICAM conformance program to verify third party credentials.

Full Assessment Team The group of individuals (government and/or contractor) tasked with conducting or providing oversight for the SCA-of a system that stores, transmits, receives, or processes NRC information. Team members may include the chief information security officer (CISO), system owner, Senior IT Security Officer (SITSO), system project manager, system ISSO, system administrator(s), and assessors. This team includes the independent assessment team.

Hybrid Control A security control that is implemented for an NRC system in part as a common control (or inherited by another system) and in part as a system-specific control. Responsibility for hybrid controls is shared. The system-specific portion of the control is the responsibility of system owners; the common or inherited portion of the control is the responsibility of the common or inherited control provider.

Independent The group of individuals (government and/or contractor) tasked with conducting or providing independent oversight of the SCA-of a system

Assessment Team that stores, transmits, receives, or processes NRC information. Team members may include the CISO, SITSO, CSO representative, assessment project manager, and assessor. This team is a subset of the full assessment team.

Individuals An assessment object that includes people applying specifications, mechanisms, or activities.

Inherited Control A security control (or portion of a security control) that is developed, implemented, assessed, authorized, and monitored by system staff other than the system staff for the inheriting system.

Interview A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.

Mechanisms An assessment object that includes specific protection related items (e.g., hardware, software, or firmware) employed within or at the boundary of a system.

Not Applicable An assessment finding indicating that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective does not apply to the assessed system per the guidance provided in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, “Security and Privacy Controls for Federal Information Systems and Organizations.”

Other than Satisfied An assessment finding indicating that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates potential anomalies in the operation or implementation of the control that may need to be addressed by the organization.

Overall Security Control Status A status that communicates the overall effectiveness of a security control based on the cumulative assessment findings for each portion of the security control. Statuses include: Satisfied, Other than Satisfied, Provided at Agency Level, Provided by <XYZ System>, Risk-based Decision, and Not Applicable.

Project Plan A document that describes the key activities and schedule required to complete the SCA-in a way that is measurable, easily understood by all members of the full assessment team, and allows for completion of the assessment within the timeframe provided in the SCA-scoping statement.

Provided at Agency Level An assessment finding indicating that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control is met by the agency. CSO-STD-0021, “Common and Hybrid Security Control Standard” constitutes evidence that the assessment objective is provided by the agency to the assessed system; CSO-STD-0020, “Organization-Defined Values for System Security and Privacy Controls” constitutes evidence that a specific value has been defined by the agency.

Provided by <XYZ System> An assessment finding indicating that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control is met by a system that is represented here as XYZ system.

A signed service level agreement between the organizations providing and inheriting the assessment objective constitutes evidence that the assessment objective is provided as a service to the assessed system.

Risk A measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk-Based Decision An assessment finding indicating that authorizing officials have accepted the risk associated with deficient assessment objectives due to the compensating controls and mitigating factors documented in a deviation approval memo or waiver approval memo per CSO-PROS-1324, “Deviation/Waiver Request Process.”

Satisfied An assessment finding indicating that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result.

Service Level Agreement A service level agreement identifies exactly what services each party will provide and the parameters surrounding those services. For example, a service level agreement may indicate that anti-malware software will be provided and that the software will be updated at least daily or that full-backups will be performed weekly at midnight on Saturday and incremental backups performed daily on all other days at midnight.

System Cybersecurity Assessment (SCA) A full assessment of a system’s security controls, including vulnerability scans and configuration checks, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The SCA-supports system authorization decisions by the DAA and provides NRC officials with the state of cyber risk associated with the system.

SCA-Package A package of documents developed by the independent assessment team to document the results of the SCA, consisting of the SCA-plan, SCA-report, and vulnerability assessment report (VAR).

The SCA-package is delivered to the project manager, the system ISSO, and the Computer Security Office (CSO) representative at the end of the assessment effort. The system ISSO must include the SCA-package as part of the authorization package when requesting an authorization to operate (ATO).

SCA-Plan A plan developed by the independent assessment team and approved by the CSO representative that describes:

- the scope of the assessment (as documented in the SCA-scoping statement);
- the approach to the assessment;
- the resources required to effectively conduct the assessment;
- the assessment timeline; and
- assumptions, constraints, or dependencies that may impact the independent assessment team's ability to effectively and thoroughly assess the system.

SCA-Report A report developed by the assessor(s) that documents the results of the SCA-and provides the assessed risk levels for all security controls with an assessment finding of "other than satisfied" or "risk-based decision," as well as any other concerns the assessor(s) identify during the SCA-.

SCA-Scoping Statement A document used to clearly and concisely identify the scope of the SCA, assumptions that need to be understood by the full assessment team and constraints that could conceivably impact the SCA-effort. For additional information please see Section 3.1.1.

Security Categorization A formal document that characterizes a system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of the system or information stored and processed by the system would have on organizational operations, organizational assets, or individuals.

Security Control Baseline The set of minimum security controls defined for a system based upon the system sensitivity level.

Security Controls The protections prescribed for a system to protect the confidentiality, integrity, and availability of the system and its information.

Security State The security status of a system based on the resources (e.g., people, hardware, software, policies) and capabilities in place to secure the system. Security related parameters impact the security state of systems including the parameters required to satisfy other security control requirements.

Security related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Severity A rating system that represents the theoretical outcome of an exploited vulnerability or weakness. Severity 1 = Critical, Severity 2 = High, Severity 3 = Moderate, Severity 4 = Low. The severity rating does not indicate the likelihood of that outcome.

Specifications An assessment object that includes document based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with a system.

System Artifacts System documentation relevant to the operations and maintenance of a system. Many of the required system artifacts document system cybersecurity controls and information.

System Information System Security Officer (ISSO) The system owner's designated representative for the security state of the system. The ISSO is the primary contact for the system during the course of the SCA-and is responsible for ensuring the independent assessment team receives required system artifacts and access to the system and personnel as required.

System Inventory All hardware and software within a system's authorization boundary at the time of the SCA-kickoff meeting.

System Security Plan (SSP) A formal document that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements.

System Sensitivity Level A categorization that reflects the highest sensitivity level of information processed by or stored on the system. Unclassified system sensitivity levels equal the highest sensitivity of information processed by or stored on the system and include low, moderate, high, and Safeguards Information (SGI). Classified system sensitivity levels equal the highest level of classified information processed by or stored on the system.

System-Specific Control A security control for an NRC system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within a system. System-specific controls are the primary responsibility of system owners.

Tailoring (Assessment Procedures) The process by which assessment procedures defined in NIST SP 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans" are adjusted, or scoped, to match the characteristics of the system under assessment, providing organizations with the flexibility needed to meet specific organizational requirements and to avoid overly constrained assessment approaches.

Test A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.

Threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Source The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Vulnerability A weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment Report (VAR) A report developed by the assessor(s) that provides a detailed summary of all vulnerabilities detected during vulnerability scans and configuration checks of system components.

Vulnerability Scan A scan of system components using an NRC approved scanning tool.

Vulnerability Severity An assessment of the relative importance of mitigating or remediating the vulnerability. The severity can be determined by the extent of the potential adverse impact if such a vulnerability is exploited by a threat source. Thus, the severity of vulnerabilities, in general, is context dependent.

2.2 References

This process was developed to align with the security control assessment process as documented in NIST SP 800-53A, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.”

Federal Information Processing Standards (FIPS) and NIST publications can be found at: http://csrc.nist.gov/.

NRC CSO requirements can be found at http://www.internal.nrc.gov/CSO/.

Additional references include, but are not limited to the following:

- Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, December 2002
- FIPS-Publication 199, “Standards for Security Categorization of Federal Information and Information Systems”

- FIPS-Publication 140 2, “Security Requirements For Cryptographic Modules”
- Executive Office of the President of the United States and Federal CIO Council, Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance
- NIST Special Publication (SP) 800-27, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security)”
- NIST SP 800-30, “Guide for Conducting Risk Assessments”
- NIST SP 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
- NIST SP 800-44, “Guidelines on Securing Public Web Servers”
- NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”
- NIST SP 800-53A, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans”
- NIST SP 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”
- NIST SP 800-82, “Guide to Industrial Control Systems (ICS) Security”
- NIST SP 800-95, “Guide to Secure Web Services”
- NIST SP 800-115, “Technical Guide to Information Security Testing and Assessment”
- NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations”
- CSO-STD-0020, “Organization-Defined Values for System Security and Privacy Controls”
- CSO-STD-0021, “Common and Hybrid Security Control Standard”
- CSO-PROS-1324, “Deviation/Waiver Request Process”
- CSO-PROS-1401, “Periodic System Scanning Process”
- CSO-PROS-2016, “Plan of Action and Milestones Process”
- CSO-PROS-2030, “NRC Risk Management Framework (RMF) and Authorization Process”
- CSO-PROC-2104, “System Artifact Examination Procedure”

3 SPECIFIC REQUIREMENTS

The following sections address the SCA-process and the actions required when conducting an SCA. SCAs require that all system artifacts required for the assessment be current, reflect the state of the system being assessed, and be official agency records (OAR) in the Agencywide Documents Access and Management System (ADAMS).

SCAs are conducted by independent assessors who have technical knowledge concerning the hardware and software components within the assessed system’s authorization boundary. Assessors must determine whether system security controls are providing the protection required for the system and whether the protection complies with NRC requirements.

Assessors also conduct vulnerability scans and configuration checks of the system components identified in an approved SCA-plan to determine whether the components are configured, operated, and maintained per federally-mandated and agency requirements. The assessment project manager serves as the primary contact on the independent assessment team. The responsible CSO SITSO must approve in writing (e.g., via email) the appointment of the assessment project manager.

SCAs are facilitated by the system ISSO, who is the primary contact for the assessed system. System ISSOs are responsible for the overall security of the system and must be familiar with the system's security state, policy, procedures, and any current issues that could pose a risk to the system or NRC. The system ISSO is also responsible for system documentation updates, completion of NRC continuous monitoring activities, and management of the system administrator's cybersecurity relevant activities.

System administrators support SCAs by being physically present during all test activities conducted during the SCA, including vulnerability scans and configuration checks of assessed hardware and software components, and providing the assessor(s) with access to all system components required to assess the system. System administrators must also be available for interviews conducted by the assessor(s) to provide details concerning the implementation of specific security controls and to provide supporting documentation (evidence) of their implementation.

CSO representatives provide oversight throughout the assessment effort and ensure that SCAs are conducted per current NRC guidance.

Figure 1 illustrates the four phases of the SCA-process.

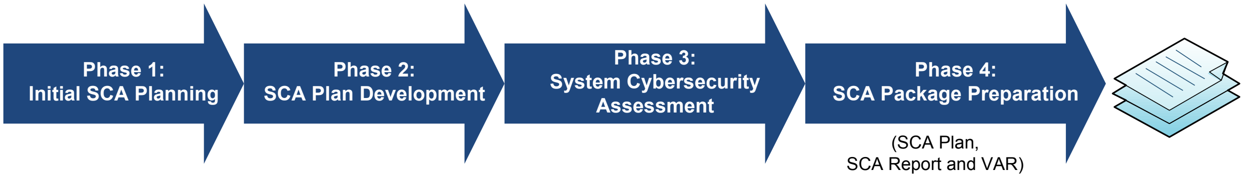


Figure 1: SCA-Process Phases

The following sections describe the phases of the SCA-process and the activities that take place during each phase.

3.1 Phase 1: Initial SCA-Planning

The SCA-must be properly planned to ensure that appropriate resources are available when needed and to ensure that the assessment can be completed in a timely manner. The following issues must be considered during the initial planning phase:

- system deadlines for cybersecurity risk management activities;
- expiration date of the system's authorization if the system was granted an authorization in the past;

- scope of the assessment;
- system inventory;
- physical location of system components (e.g., NRC Headquarters, regional sites, non NRC facilities, etc.);
- contractor or outsourced vendor experience with, commitments to, and environment supporting the appropriate and verifiable handling of agency required security controls
- resources and skills required for the assessment, including independent assessment team members
- current state (e.g., current, out of date) of supporting system artifacts (e.g., system security plan (SSP), system-specific policies and procedures, etc.);
- whether any controls have been tailored based on the system's confidentiality, integrity, and availability requirements; and
- operational issues related to system availability and critical system timeframes that must be avoided.

Initial SCA-planning involves the steps illustrated in Figure 2.

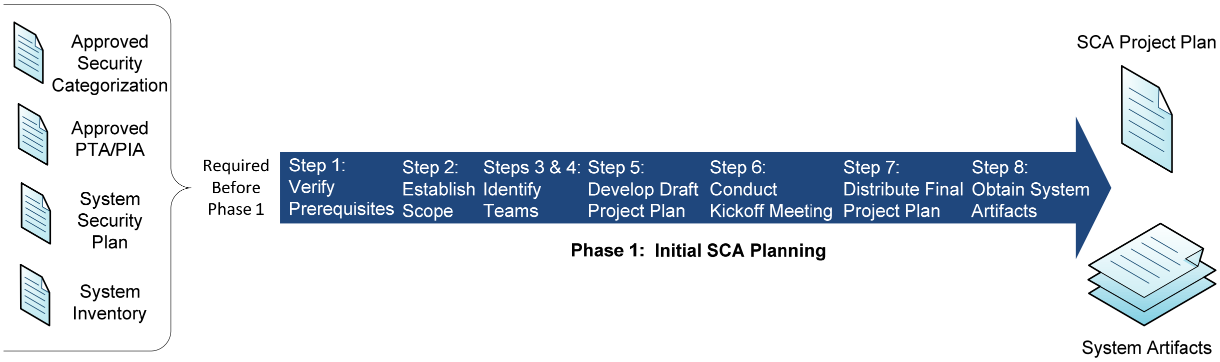

Approved Security Categorization
Approved PTA/PIA
System Security Plan
System Inventory
Required Before Phase 1
Step 1: Verify Prerequisites
Step 2: Establish Scope
Steps 3 & 4: Identify Teams
Step 5: Develop Draft Project Plan
Step 6: Conduct Kickoff Meeting
Step 7: Distribute Final Project Plan
Step 8: Obtain System Artifacts
Phase 1: Initial SCA Planning
SCA Project Plan
System Artifacts

Figure 2: Initial SCA-Planning

A.1.1 PREREQUISITES

Prior to beginning SCA-activities, the CSO representative and assessment project manager must verify that the following prerequisite activities have taken place:

- The system security categorization has been reviewed and approved by CSO.
- The system privacy threshold analysis (PTA) and privacy impact assessment (PIA) (if privacy information is processed) have been reviewed and approved by the Office of Information Services (OIS) Customer Service Division, Freedom of Information Act (FOIA), Privacy, and Information Collection Branch.
- The SSP has been developed and documents:
  - the implementation of each security control within the system's security control baseline, and

  - the rationale for security controls that were tailored out of or added to the baseline to more closely align with the organization's mission and business requirements and the system's environment of operation.

- The system inventory is accurate, complete, and up to date.

If any of the above conditions have not been met, the SCA-must be postponed.

3.1.1 Scope

Once the CSO representative and the assessment project manager have verified the SCA-prerequisite activities, establishing the scope for the assessment is the next step in the initial SCA-planning phase. The system ISSO shall discuss the current state of the system with the system project manager, CSO representative, and the assessment project manager for the purpose of establishing the scope of the assessment.

Once the scope of the assessment is agreed upon, the assessment project manager or designee shall develop the draft SCA-scoping statement and distribute it to the system project manager, the system ISSO, and CSO representative. The system project manager, system ISSO, and CSO representative shall notify the assessment project manager in writing of their concurrence of the scope of the assessment. The SCA-scoping statement must:

- Clearly identify the assessment boundary, from which the independent assessment team will select a sample of system components for vulnerability scans and configuration checks per the sampling requirements stated in CSO-PROS-1401.
- Address the tailoring of assessment procedures to match the characteristics and sensitivity level of the system to be assessed and the system's environment of operation, if applicable.
- Specify the timeframes for completing the assessment, including timeframes for conducting vulnerability scans and configuration checks (see Section 3.3.3.2 for more details).
- Specify dependencies along with potential impacts.

3.1.2 Independent Assessment Team

After obtaining concurrence on the scope of the SCA, the assessment project manager must identify the independent assessment team members and must communicate the membership to the responsible CSO SITSO, the system project manager, and the system ISSO. The independent assessment team shall consist of:

- **Assessment Project Manager.** The individual responsible for overseeing the development and distribution of the assessment project plan, and for revising the plan if necessary during the course of the assessment. The assessment project manager serves as the primary contact for issues that may impact or delay key assessment activities.
- **Assessor(s).** The assessor(s) shall be identified by the assessment project manager, and communicated to the CSO representative, the system project manager, and system ISSO. The communication must include evidence of required skillsets. The assessors selected for the SCA-must:
  - Possess the baseline skillsets for review, target identification, and analysis techniques established in NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment."

  - Be independent[1]and must not serve in a support role for the system being assessed (e.g., as an ISSO, system administrator, or system documentation developer.)
  - Be knowledgeable of NRC cybersecurity policy, standards, and procedures.
  - Be experienced with NRC approved vulnerability scanning tools and methods for testing the security configurations of system network devices, servers, and workstations to determine whether they comply with NRC configuration standards.
  - Be authorized by CSO and the Office of Information Services (OIS) (or the system ISSO for assessments of systems hosted in non-NRC facilities) to conduct configuration checks and vulnerability scans. This authorization is performed using the System Periodic Scanning Tools Authorization Form provided in CSO-PROS-1401.
- **CSO Representative.** The CSO representative shall be identified by the CSO SITSO responsible for SCAs.

3.1.3 Full Assessment Team

The full assessment team must also be identified prior to the SCA-kickoff meeting. At a minimum, the full assessment team shall consist of:

- **Independent Assessment Team.** The independent assessment team is identified by the assessment project manager.
- **System Project Manager.** The project manager is the system owner's representative to run the system project requiring the assessment.
- **System ISSO.** The system ISSO is formally appointed by the system owner.
- **System Administrator(s).** The system administrator supporting the assessed system shall be identified by the system ISSO and communicated to the CSO representative and assessment project manager prior to the SCA-kickoff meeting.

3.1.4 Draft SCA-Project Plan and SCA-Project Kickoff

The project plan must identify the key activities required to complete the SCA-in a way that is measurable, easily understood by all members of the full assessment team, and allows for completion of the assessment within the timeframe provided in the SCA-scoping statement. The assessment project manager shall ensure the draft project plan is completed within five (5) business days after establishing the scope and receiving a full and accurate system inventory, and shall distribute the project plan to all full assessment team members.

The assessment project manager or designee shall schedule a kickoff meeting at least five (5) business days before the day of the meeting and within five (5) business days of submitting the draft project plan. Prior to or as part of scheduling the meeting, the assessment project manager shall provide electronically a list of system artifacts (along with the dates that the artifacts are due to the independent assessment team) that are required at a minimum before beginning the assessment. The kickoff meeting shall be attended by the full assessment team, including the assessor(s), the system project manager, the system ISSO, system administrator(s), the assessment project manager, and the CSO Representative.

[1] Per NIST SP 800-37, an independent assessor is any individual or group capable of conducting an impartial (no vested interest in the outcome) assessment of security controls employed within or inherited by a system.

The following topics must be discussed during the meeting:

- **Full Assessment Team members.** All team members shall be introduced, and each member's role on the team shall be stated.
- **Scope of the assessment.** The scope of the assessment shall be discussed, and a copy of the SCA-scoping statement shall be distributed to team members.
- **Draft Project Plan.** The draft project plan and key assessment milestones shall be reviewed, and any issues identified that might impact the schedule or put the project at risk shall be discussed. If it is not possible to conduct the required assessment per the timeframe supplied in the draft project plan, the assessment project manager, CSO representative, the system project manager, and system ISSO shall discuss viable options, and adjust the plan accordingly.
- **System access.** The assessor(s), the system project manager, system ISSO, and system administrators shall discuss logistical requirements for conducting vulnerability scans and configuration checks. Concerns about the sensitivity of specific components to vulnerability scans, or a lack of credentials must be discussed (e.g., for vendor supported components). The system project manager, system ISSO, system administrator(s), and assessor(s) shall discuss the availability of system staff for Interviews that will be conducted by the assessor(s) to obtain insight into how the system operates and determine where to find specific information needed for the assessment.
- **System artifacts.** The independent assessment team shall also lead a discussion to determine the current state of system artifacts. The list of system artifacts required may be expanded as the assessment team reviews any initial documentation received and additional documentation needs are discovered.
- **System Overview.** In order to assess the system it is essential that the assessors and project team fully understand the target system being assessed as well as its business mission, purpose, design, architecture, components and risks.
- **Questions and concerns.** The full assessment team members shall discuss any questions or concerns that they may have as it relates to the status of the system, CSO guidance, the SCA-process, or other issues (e.g., the impact of pending system changes on the assessment effort).

3.1.5 Final Project Plan

The independent assessment team shall finalize the project plan per any concerns discussed and resolved during the kickoff meeting, and shall distribute the final project plan to the full assessment team.

3.1.6 Required System Artifacts

Before the SCA-plan is developed, system project manager must ensure the system ISSO provides supporting system artifacts to the independent assessment team within three (3) business days of the final project plan being distributed. All artifacts used must be OARs, ADAMS accession numbers must be provided for the artifacts electronically via NRC eMail, and the assessment team must be granted access to the documents. These artifacts provide the information required to ensure that the security controls and hardware components selected for the assessment, and the tools selected to conduct vulnerability scans and configuration checks, reflect current CSO SCA-requirements.

A delay in providing system artifacts to the independent assessment team exceeding three (3) business days will result in a delay in the assessment. Assessment resources support multiple systems; therefore, re scheduled assessments must be scheduled when the required resources are available.

System artifacts must be up to date and must accurately reflect the current as built state and security state of the system. Information provided in these documents allows the independent assessment team to develop a comprehensive, accurate SCA-plan. Out of date, inaccurate system artifacts cause confusion, and could potentially result in:

- an inaccurate assessment of specific security controls, and associated risks;
- an inaccurate assessment of system hardware or software components; or
- reassessment of security controls or system components upon receiving accurate information, which ultimately increases the system owner assessment costs and the length of time required to perform the assessment. For details concerning the evaluation of each artifact, see CSO-PROC-2104, “System Artifact Examination Procedure.”

In some instances, the independent assessment team may determine that the artifacts are so out of date that the assessment cannot be performed until the artifacts are updated to reflect the current state of the system. In those cases, the assessment must be cancelled and rescheduled to take place after the artifacts are updated. If this is necessary, the system owner will incur the cost of work performed to that point as well as the cost to perform a full assessment at a later date.

The system ISSO must provide the following system artifacts (most current version including the ADAMS accession number[2]) to the independent assessment team within three (3) business days of the final project plan being distributed:

- System security categorization
- SSP that reflects the current as built state and security state of the system. The SSP must:
  - Provide a security control baseline for the system (including any security control tailoring).
  - Describe how the security controls are implemented within the system.
  - Provide the rationale for tailoring security controls in the security control baseline to more closely align with the organization’s mission and business requirements and the system’s characteristics and environment of operation.
  - Include an authorization boundary diagram that illustrates the current as built state of the system, including any interconnected and/or dependent systems and services.
  - Reflect information obtained during the most recent continuous monitoring activities (e.g., periodic vulnerability scans as documented in the last quarter’s periodic scan report, the last quarter’s Plan of Action and Milestones [POA&M] updates, any new or updated artifacts (i.e., plans, diagrams) for any security controls or components, penetration test reports, or configuration audit results, etc.).

[2] ADAMS accession numbers allow the independent assessment team to cite OARs throughout SCA-package deliverables. This enables all SCA-stakeholders to review related system artifacts if necessary.

- A hardware inventory reflecting the current as built state of the system, listing every hardware component within the system's authorization boundary. At a minimum, the inventory must provide the information required for the CM-8 control in NIST SP 800-53, and CSO-STD-0020 and include the following information:
  - Servers and workstations. The inventory must provide each component's host name, IP address, role/purpose, vendor, model, and operating system, including the operating system version (e.g., Windows 2008 R2 or Red Hat Enterprise Linux Version 5). The inventory must also specify whether the device hosts any virtual machines and the nature (i.e., operating system, role/purpose, etc.) of the virtual machines. The physical location of the component (i.e., site, building, and room number) must also be provided.
  - Mobile devices. The inventory must provide each device's role/purpose, vendor, model, and operating system, including the operating system version (e.g., Blackberry Operating System (OS) version 3.6, etc.).
  - Network devices. The inventory must provide each network component's host name, IP address, role/purpose, vendor, model, and operating system, including the operating system version (e.g., Cisco IOS Release 12.2 or Juniper Junos 9.4).
- A software inventory reflecting the current as built state of the system, listing every software component, including operating system, installed on every hardware component within the system's authorization boundary (e.g., Windows 2008 R2, Microsoft Exchange, Internet Information Services [IIS], or SQL Server). At a minimum, the inventory must provide the information required for the CM-8 control in NIST SP 800-53 and CSO-STD-0020 and include the following information:
  - The product name, version, vendor, license number, number of licenses, license expiration date, and the host name of every hardware component that the software is installed on.
  - The function or purpose of the software on each hardware component.
- Assessment reports (annual security control test reports, annual security control and vulnerability test reports, VARs, Penetration Tests, Office of the Inspector General [OIG] audits) for the previous two (2) years if the system was granted an authorization in the past.
- Security impact analysis (SIA) and change assessments for the previous three (3) years (if the system was granted an authorization in the past and SIAs and/or change assessments were conducted).
- Configuration management plan
- System contingency plan
- Contingency test plans and contingency test reports for the previous two (2) years (if the system was granted an authorization in the past).
- The system POA&M, exported from the NRC information assurance tool on the day of the SCA-kickoff meeting.
- All deviation requests
- Deviation approval memos, issued by the NRC DAA
- All waiver requests
- Waiver request approval memos, issued by the NRC DAA

- Authorization approval memo (issued by the NRC DAA if the system was granted an authorization in the past)
- Security Assessment Report (SAR) or SCA-report (submitted to the NRC DAA if the system was granted an authorization in the past)
- System architecture document (SAD)
- Business impact analysis (BIA)
- Incident response plan
- Privacy threshold analysis (PTA)
- Privacy impact assessment (PIA)
- Signed service level agreements (SLA), and/or supporting contract documentation
- Signed memoranda of understanding (MOU)
- Signed interconnection security agreements (ISA)
- System-specific policies and procedures
- Operations guide/administrator guides
- Access/inventory/audit logs
- Reports providing current configuration settings
- Vulnerability Assessment Reports (VAR)
- Meeting minutes concerning activities related to assessment objectives

In addition, the system ISSO must provide any other artifacts that apply to the system to the independent assessment team. The most current version (including the ADAMS accession number) must be provided. These artifacts are reviewed to determine whether or not the associated assessment objective is satisfied.

3.2 Phase 2: SCA-Plan Development

After all activities in the initial SCA-planning phase are complete, the independent assessment team is responsible for developing a SCA-plan using the CSO template. The plan must identify the scope of the assessment, all full assessment team members, and the NRC approved vulnerability scanning tools and configuration standards to be used during the course of the assessment.

SCA-Plan Development involves the steps illustrated in Figure 3.

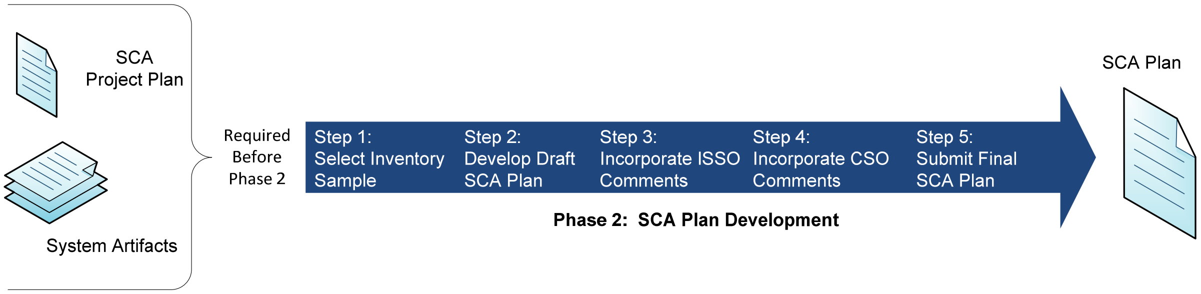

SCA Project Plan
System Artifacts
Required Before Phase 2
Step 1: Select Inventory Sample
Step 2: Develop Draft SCA Plan
Step 3: Incorporate ISSO Comments
Step 4: Incorporate CSO Comments
Step 5: Submit Final SCA Plan
Phase 2: SCA Plan Development
SCA Plan

Figure 3: SCA-Plan Development

3.2.1 Select System Inventory Sample

The independent assessment team must select a sample of the system inventory for vulnerability scans and configuration checks. The sample must meet or exceed the guidelines outlined in CSO-PROS-1401. The assessment project manager or designee must submit the proposed sample to the CSO representative and obtain sample approval before the plan is approved. The sample selection must only be known to the independent assessment team and the CSO representative until 2 business days prior to the scan at which time the ISSO is notified of the selection.

3.2.2 Develop Draft SCA-Plan

The independent assessment team shall develop a draft SCA-plan to ensure that all full assessment team members and SCA-stakeholders understand the scope of the assessment (as documented in the SCA-scoping statement). The plan must address the approach to the assessment, the resources required to effectively conduct the assessment, and any assumptions, constraints, or dependencies that may impact the independent assessment team's ability to effectively and thoroughly assess the system.

When developing the SSP, organizations can tailor the security control baseline based on unique system characteristics and the system's environment of operation. The independent assessment team must ensure that the SCA-Plan is developed in consideration of the system's tailored security control baseline.

The draft SCA-Plan must specify:

- the system's impact levels for confidentiality, integrity, and availability as stated in the system's approved security categorization;
- procedures that provide sufficient detail such that a technically trained individual, not familiar with the system, can successfully follow the procedures to ensure that all federally-mandated and NRC-defined security requirements are fully tested;

  These procedures must specifically describe how all assessment objects will be evaluated, how all components will be tested, and how the assessment procedures have been tailored to match the characteristics and environment of the system to be assessed.
- any assumptions, constraints, or dependencies that may affect the assessment;

- information concerning vulnerability scans of system components, including:
  - the NRC approved vulnerability scanning tools that will be used during the course of the assessment;
  - A list of all internal (CSO standards) and external (Defense Information Systems Agency [DISA] Security Technical Implementation Guides [STIGs] or Center for Internet Security [CIS] Benchmarks) configuration standards to be used during configuration checks of system components; and

    The configuration standards that were in effect on the date of the assessment kickoff meeting must be used.
  - automated scan results that may be acceptable instead of performing another scan.

The draft SCA-Plan must also explain that the system's baseline security controls will be assessed in accordance with the current version of the following:

- NIST SP 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans"
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
- NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"
- CSO-PROS-1324, "Deviation/Waiver Request Process"
- CSO-PROS-1401, "Periodic System Scanning Process"
- CSO-PROS-2016, "Plan of Action and Milestones Process"
- CSO-STD-0020, "Organization-Defined Values for System Security and Privacy Controls"
- CSO-STD-0021, "Common and Hybrid Security Control Standard"
- CSO-PROC-2104, "System Artifact Examination Procedure"
- CSO Web Page (http://www.internal.nrc.gov/CSO/) for policies, standards, processes, procedures, templates and guidance other than those specifically listed.

3.2.3 Obtain and Incorporate System ISSO and CSO Feedback

After the draft SCA-plan is developed, the independent assessment team shall submit the plan to the system project manager, system ISSO, and CSO for review. The copy of the plan sent to the system project manager and system ISSO must not specify the system inventory sample selected for vulnerability scans and hardening checks. The system project manager and system ISSO shall review the plan and provide feedback to the independent assessment team and CSO within ten (10) business days of receipt of the draft plan. If no feedback is provided within that timeframe, the plan will be considered acceptable to the system ISSO.

If the system project manager or system ISSO provides feedback on the draft SCA-plan, the independent assessment team shall review and consider the feedback, coordinate any requested changes with the CSO representative, and update the SCA-plan within five (5) business days of receipt of feedback.

3.2.4 Submit the Final SCA-Plan to the System ISSO and CSO

After feedback from the system project manager and system ISSO is incorporated into the SCA-plan, the assessment project manager or designee must provide the final SCA-plan to the system project manager, system ISSO and the CSO representative for a ten (10) business day review and approval period. The copy of the plan sent to the system project manager and system ISSO must not specify the system inventory sample selected for vulnerability scans and hardening checks

During this time, the system project manager, system ISSO, CSO representative, and/or CSO SITSO may provide additional comments and may request additional updates to the plan. The independent assessment team shall incorporate the feedback provided during this period into the SCA-plan. If the plan is updated, the assessment project manager or designee must provide the updated plan to the system project manager, system ISSO, and CSO representative.

No later than the end of the ten (10) business day review period, CSO shall notify the independent assessment team that the SCA-plan is approved, and authorize the independent assessment team to begin the assessment.

3.3 Phase 3: System Cybersecurity Assessment

The assessor(s) must use the approved SCA-plan to independently determine how effectively the system complies with all federal and NRC mandated cybersecurity requirements for the system's security control baseline.

In order to effectively assess the system's security controls, the assessor(s) must first gather certain system-specific background information. At a minimum, assessor(s) must determine the background information described in Appendix A of this process.

The assessor(s) must assess each security control using the assessment objects, procedures, and methods described in NIST SP 800-53A, as well as those required by NRC policy and standards.

SCAs involve activities conducted using each of the assessment methods illustrated in Figure 4.

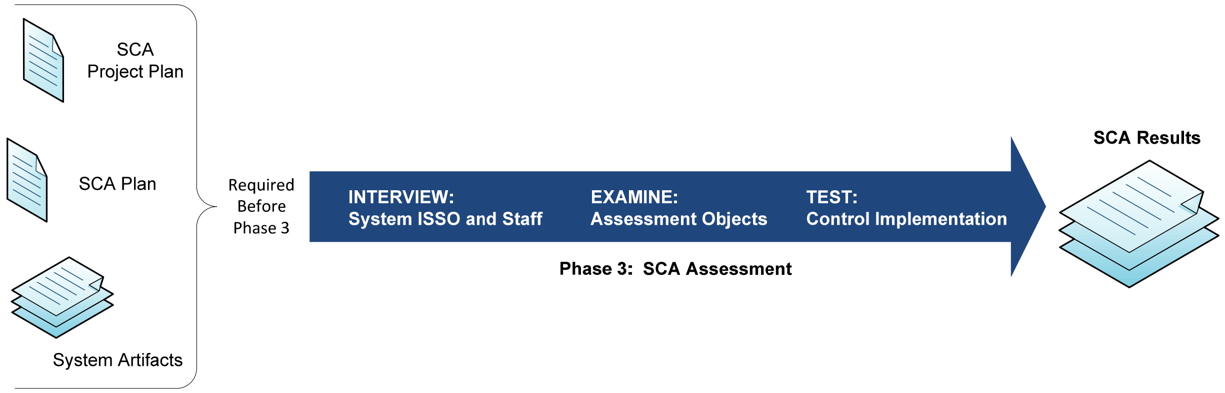


Figure 4: SCA-Assessment

3.3.1 Interview System Personnel

The assessor(s) must conduct interviews with the system ISSO, system administrators, and system support staff to obtain a complete understanding of the system, determine where to find specific information needed for the assessment, and obtain clarification concerning specific assessment objects. At a minimum, the assessor(s) shall ask the interview questions provided in Appendix B of this process. The rigor and scope (depth and coverage) applied to each interview shall be commensurate with the assurance requirements associated with the evaluated impact level to each security objective (confidentiality, integrity, and availability) as documented within the system's security categorization (see NIST SP 800-53A for more details).

Assessors must also ask for additional information as warranted by replies to the interview questions. Answers shall be evaluated based on currently effective cybersecurity guidance and the NRC defined values within CSO-STD-0020.

Statements made during interviews shall not be used as evidence of the implementation of a control; the statements shall be used simply to "facilitate understanding, achieve clarification, or identify the location of evidence."[3] Interview information does not in itself constitute the evidence required.

3.3.2 Examine Assessment Objects

Assessor(s) must examine various assessment objects during the course of the SCA-to determine whether specific assessment objectives are satisfied and comply with federal and NRC standards. This includes reviewing system artifacts (e.g., ensuring system-specific procedures are available and up to date). Assessment objects to be reviewed also include system files, rule sets, audit logs, etc. for the purpose of identifying evidence that an assessment objective is or is not satisfied. Assessor(s) shall cite all evidence supporting the status of each assessment objective in the SCA-report.

[3] NIST SP 800 115, Technical Guide to Information Security Testing and Assessment

At a minimum, the assessor(s) shall conduct the examination activities provided in Appendix B of this process. The rigor and scope (depth and coverage) applied during the examination of assessment objects shall be commensurate with the assurance requirements associated with the evaluated impact level to each security objective (confidentiality, integrity, and availability) as documented within the system's Security Categorization (see NIST SP 800-53A for more details).

The examination activities in Appendix B must be conducted for every applicable component within the sample selected for the assessment. For example, if more than one system component contains unique user accounts (e.g., operating system accounts, application accounts, database accounts, etc.), all account management examination criteria must be evaluated for each type of unique account. If the assessor(s) identify a finding for any component of the system or any account, then they must indicate that the AC-2 control is other than satisfied (deficient), and assign a risk level.

Assessment objects shall be evaluated based on currently effective cybersecurity guidance and the NRC defined values within CSO-STD-0020.

3.3.2.1 Deficient System Artifacts

Deficiencies and discrepancies in assessed system artifacts must be identified in the SCA-report. For example, if an SSP provides little to no detail concerning the implementation of system security controls, the assessor must indicate that the PL-2 control is other than satisfied (deficient). See CSO-PROC-2104, "System Artifact Examination Procedure" for details on assessing system artifacts.

3.3.3 Test Control Implementation

The assessor(s) shall arrange times to test specific assessment objectives for each applicable security control. When testing the assessment objectives, the assessor(s) shall look for evidence that the assessment objective is or is not satisfied based on actual behavior (as opposed to documented behavior).

Before testing, the assessor(s) must ensure that security controls provided at the agency level, in whole or in part, are truly applicable to the assessed system per CSO-STD-0021, "Common and Hybrid Security Control Standard" and the supporting SSP. If they are applicable, the assessor(s) shall not test them; CSO conducts annual assessments of NRC wide (common) controls.

During testing, the assessor(s) must maintain detailed notes concerning the actual behavior of each tested assessment objective. In addition to the notes, evidence supporting the test result (e.g., audit logs, access control lists, configuration settings, vulnerability scan results, and documented system level policies and procedures) must be added, when possible, to an electronic repository created for the purpose of storing assessment artifacts and evidence.

3.3.3.1 Test Activities

At a minimum, the assessor(s) shall perform the test activities described in Appendix B of this process. The rigor and scope (depth and coverage) applied to each test activity shall be commensurate with the (NIST and NRC minimum) assurance requirements associated with the evaluated impact level to each security objective (confidentiality, integrity, and availability) as documented within the system's security categorization (see NIST SP 800-53A for more details).

The test activities in Appendix B must be conducted for every applicable component within the sample selected for the assessment. For example, if more than one system component contains unique user accounts (e.g., operating system accounts, application accounts, database accounts, etc.), all account management test criteria must be evaluated for each type of unique account. If the assessor(s) identify a finding for any component or any account of the system, then they must indicate that the AC-2 control is other than satisfied (deficient), and assign a risk level.

The test activities shall be evaluated based on currently effective federal and NRC cybersecurity guidance and the NRC defined values within CSO-STD-0020.

3.3.3.2 Conduct System Vulnerability Scans and Configuration Checks

As part of testing the system, assessor(s) must conduct vulnerability scans and security configuration checks of the system components identified in the SCA-plan to determine whether the components are configured, operated, and maintained per federally-mandated and NRC requirements. This includes the following types of scans and checks per CSO-PROS-1401.

- **Vulnerability Scans:** The NRC approved vulnerability scanning tools all implement the federal government’s Security Content Automation Protocol (SCAP) standard by implementing Common Vulnerability Enumeration (CVE), Common Platform Enumeration (CPE), and the Common Vulnerability Scoring System (CVSS).
  - Automated Vulnerability Scans: If automated vulnerability scanning is implemented for the assessed system (e.g., using Tenable or a similar tool), the independent assessment team must formally request authorization in writing (e.g., via email) from the CSO Representative to pull scan results for the system.
  - Manual Vulnerability Scans: If the independent assessment team is conducting vulnerability scans (e.g., manual Nessus scans), the independent assessment team must formally request authorization in writing from the CSO Representative to scan system components.
- **Configuration Checks:** System component configuration settings will be examined and compared to the settings required in internal or, if applicable, external CSO configuration standards. Currently effective standards are listed on the CSO standards page at http://www.internal.nrc.gov/CSO/standards.html.

Vulnerability scans and configuration checks shall be scheduled to align with the dates established in the published SCA-project plan, and the independent assessment team and system ISSO shall coordinate activities to minimize disruption to the organization.

The timeframe for conducting vulnerability scans and configuration checks of system components will vary based on the factors below:

- the type of vulnerability scans conducted (automated or manual);
- the number of system servers, network devices, and workstations in the selected inventory sample; and
- the number of platforms and applications for which configuration checks need to be conducted.

The ISSO must inform CSO and the assessor if there are any special conditions related to scanning. For example, if 2 specific components cannot be scanned at the same time (must be scanned at different times or in sequence) due to operational impact, this information must be provided prior to development of the scanning plan.

The assessment project manager, CSO representative, and system ISSO shall discuss and agree to the timeframe for conducting vulnerability scans and configuration checks during development of the SCA-scoping statement, and this timeframe must be reflected in the SCA-project plan and SCA-plan.

Summarize Vulnerability Scan and Configuration Check Results

The assessor(s) shall review and analyze the raw scan results to identify known false positives and approved deviations or waivers that may apply to the vulnerabilities. The assessor(s) shall review the tool provided remediation recommendations for accuracy and to ensure that each recommendation provides sufficient information for a system administrator to remediate the vulnerability using the recommendation. If the tool provided recommendation is not accurate or does not provide sufficient information, the assessor(s) will augment the recommendation to ensure that it is useful and actionable.

After the raw scan results are analyzed, the assessor(s) shall transfer the results into the CSO Findings Tracking Sheet (FTS) Excel template. The template provides columns for the vulnerability ID, the tool generated description of the vulnerability, the hosts affected by the vulnerability, the severity of the vulnerability, a recommendation for remediating the vulnerability, and the root cause of the vulnerability (e.g., missing patches or noncompliant configuration settings). The template also provides a column for tracking the status of each vulnerability (open, or closed), and a column to enter notes concerning the status of the vulnerability or remediation activities.

Within the FTS, for each vulnerability scanning tool and configuration standard used during vulnerability scans and configuration checks, the assessor(s) shall create a worksheet listing all identified vulnerabilities for the tool or configuration standard, and a separate worksheet listing all known false positives identified for the tool or standard.

Supporting rationale for each false positive must be provided (e.g., IPv6 is not enabled, read only access is permitted, or the organization has an approved deviation or waiver for a configuration setting). If an approved deviation or waiver is cited as rationale for the false positive, the ADAMS accession number for the associated DAA approval memo must be provided.

Submit FTS to System ISSO

The independent assessment team shall submit the FTS to the system project manager, system ISSO and CSO representative via email along with supporting raw scan results.

The timeframe for remediating vulnerabilities may vary based on the factors below:

- the number of system servers, network devices, and workstations for which vulnerabilities were identified; and
- the number of platforms and applications for which vulnerabilities were identified.

Based on the factors above, the system project manager and system ISSO shall have no longer than 15 business days to remediate identified vulnerabilities before a follow up scan must be completed in accordance with CSO-PROS-1401.

Verify Evidence of Remediation

The independent assessment team shall contact the system project manager and system ISSO five (5) business days prior to the end of the remediation period. If follow up scans are required, the independent assessment team, system project manager, and the system ISSO shall schedule scanning to take place at the end of the remediation period.

The independent assessment team shall conduct follow up scans and manual checks to confirm that vulnerabilities identified during initial vulnerability scans have been remediated (as communicated by the system ISSO) in accordance with CSO-PROS-1401.

3.3.4 Assign Assessment Findings

NIST SP 800-53A provides assessment objectives, consisting of determination statements, for each security control. A determination statement expresses a desired outcome for the assessment of a security control or control enhancement. An example of a determination statement might be:

Determine if the organization implements separation of duties through assigned information system access authorizations.

When assessing security controls, assessor(s) shall use the interview, examine, and test methods to compile or produce the evidence required to determine whether the portion of the security control addressed by the determination statement is satisfied, other than satisfied, provided by another system, provided by the agency, not applicable, or a risk-based decision.

The assessor(s) shall then assign an assessment finding to each portion of the security control per the criteria provided in Table 1.

Table 1: Assessment Findings

Finding	Description
Satisfied	Indicates that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result.
Other than Satisfied	Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates potential anomalies in the operation or implementation of the control that may need to be addressed by the organization.
Risk-based Decision	Indicates that the NRC DAA has accepted the risk associated with a deficient portion of a security control due to compensating controls and mitigating factors documented per the CSO-PROS-1324, “Deviation/Waiver Request Process.” A signed deviation or waiver approval memo that the assessors

Table 1: Assessment Findings

Finding	Description
	determine is still valid constitutes evidence that the NRC DAA has accepted the risk associated with the deficient assessment objective.
Provided at Agency Level	Indicates that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control is provided by the NRC for the system. CSO-STD-0021, “Common and Hybrid Security Control Standard” and the supporting SSP constitute evidence that the assessment objective is provided by the NRC to the assessed system.
Provided by <XYZ System>	Indicates that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control is provided by system XYZ for the assessed system. A signed, currently effective service level agreement between the organizations providing and inheriting the assessment objective constitutes evidence that the assessment objective is provided as a service to the assessed system. Systems owned by the same organization are not required to have a service level agreement.
Not Applicable	Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates that the assessment objective is not applicable to the assessed system per the scoping guidance provided in NIST SP 800-53, “Recommended Security Controls for Federal Information Systems and Organizations.” For example, a security control that refers to a specific technology (e.g., wireless) is only applicable if wireless is employed within the assessed system, and an agency common control is not within the scope of the system and/or providing the control function.

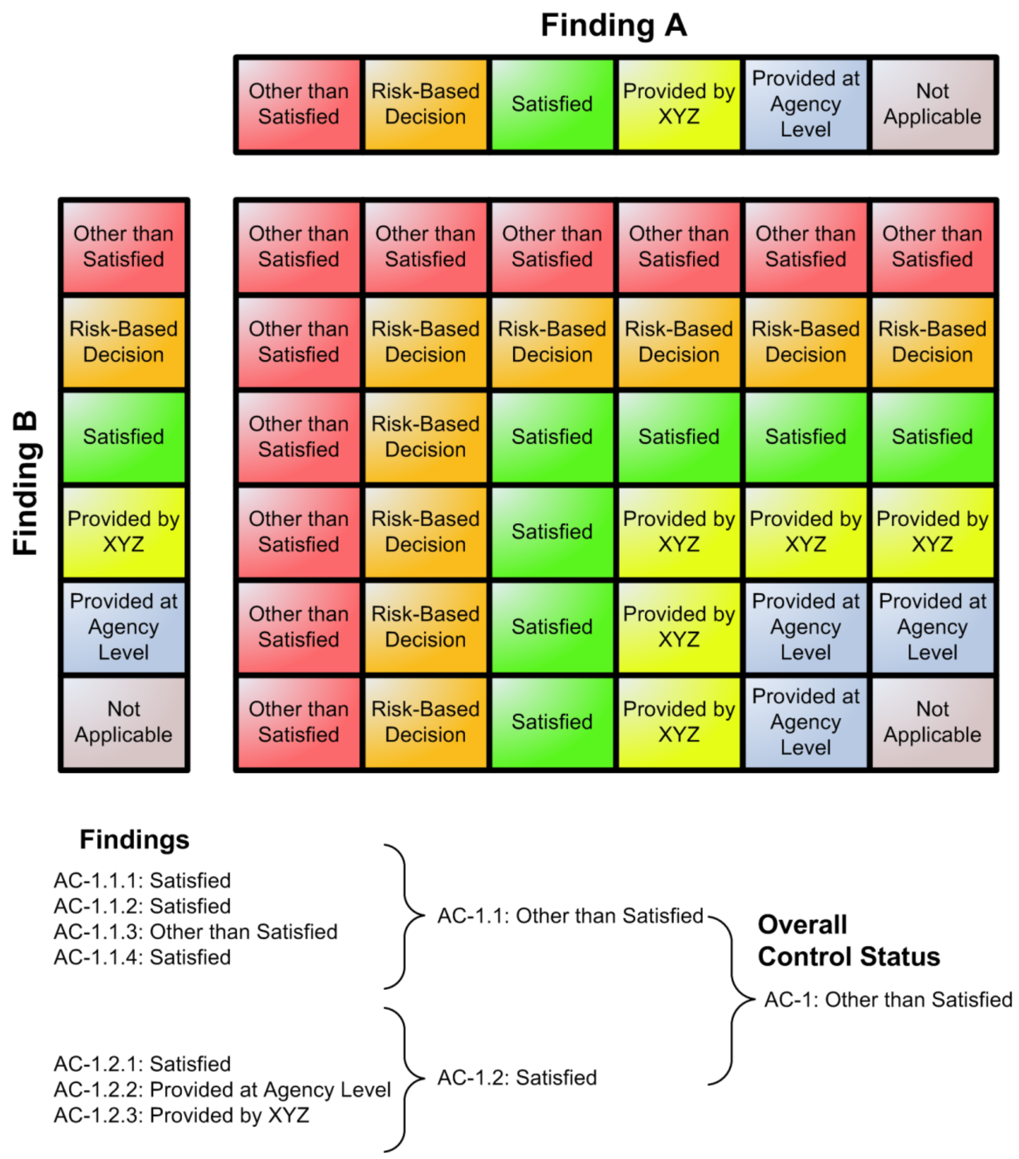
The assessor(s) document the assessment findings for assessment objectives in the SCA-report. Section 3.4.1 describes the process for developing the SCA-report. Appendix C of this process provides examples of documented assessment findings.

3.3.5 Determine Overall Security Control Status

After assigning an assessment finding to each portion of the security control, the assessor(s) must provide a status that communicates the overall effectiveness of the security control. Figure 5 provides a decision table to be used as a tool when determining the overall status of each assessed security control (and enhancement), and an example illustrating use of the decision table to determine the overall status of the AC-1 security control.

To use the table, locate the box with the status of the first finding on the Finding A axis, then locate the box with the status of the second finding on the Finding B axis. The box in the table where the Finding A column and Finding B row intersect provides the overall status of the control.

For example, if the assessor(s) find one portion of the security control to be Other than Satisfied (Finding A) and another portion to be Satisfied (Finding B), the overall status of the security control is Other than Satisfied (as indicated by the status where Finding A and Finding B intersect).



Finding B \ Finding A	Other than Satisfied	Risk-Based Decision	Satisfied	Provided by XYZ	Provided at Agency Level	Not Applicable
Other than Satisfied	Other than Satisfied	Other than Satisfied	Other than Satisfied	Other than Satisfied	Other than Satisfied	Other than Satisfied
Risk-Based Decision	Other than Satisfied	Risk-Based Decision	Risk-Based Decision	Risk-Based Decision	Risk-Based Decision	Risk-Based Decision
Satisfied	Other than Satisfied	Risk-Based Decision	Satisfied	Satisfied	Satisfied	Satisfied
Provided by XYZ	Other than Satisfied	Risk-Based Decision	Satisfied	Provided by XYZ	Provided by XYZ	Provided by XYZ
Provided at Agency Level	Other than Satisfied	Risk-Based Decision	Satisfied	Provided by XYZ	Provided at Agency Level	Provided at Agency Level
Not Applicable	Other than Satisfied	Risk-Based Decision	Satisfied	Provided by XYZ	Provided at Agency Level	Not Applicable

Findings
AC-1.1.1: Satisfied
AC-1.1.2: Satisfied
AC-1.1.3: Other than Satisfied
AC-1.1.4: Satisfied
AC-1.1: Other than Satisfied
AC-1.2.1: Satisfied
AC-1.2.2: Provided at Agency Level
AC-1.2.3: Provided by XYZ
AC-1.2: Satisfied
Overall Control Status
AC-1: Other than Satisfied

Figure 5: Security Control Status Decision Table

Table 2 provides rationale supporting each overall security control status.

Table 2: Overall Security Control Status Rationale

Status	Rationale
Satisfied	Indicates that every applicable portion of the security control has been satisfactorily implemented. Portions of a satisfied security control may be implemented at the NRC level (if CSO-STD-0021, “Common and Hybrid Security Control Standard” and the supporting SSP state that the assessment objective is provided by the NRC at the agency level), by another system (if a signed service level agreement is in place), or not applicable.
Other than Satisfied	Indicates that one or more portions of the security control are other than satisfied. As a result, anomalies in the operation or implementation of the security control need to be addressed by the organization.
Risk-based Decision	Indicates that one or more portions of the security control is deficient, and the NRC DAA has accepted the risk after reviewing the compensating controls and mitigating factors documented in a Deviation Request or Waiver Request per CSO-PROS-1324, “Deviation/Waiver Request Process.” Accepting the risk posed to the system, organization, and NRC does not satisfy the requirements of the security control; therefore, the risk must be communicated in the overall security control status.
Provided at Agency Level	Indicates that every portion of the security control is provided by the NRC at the agency level, as documented in CSO-STD-0021, “Common and Hybrid Security Control Standard,” and the supporting SSP.
Provided by <XYZ System>	Indicates that every portion of the security control is provided by another system (XYZ), as documented in a signed, currently effective service level agreement. Systems owned by the same organization are not required to have a service level agreement.
Not Applicable	Indicates that every portion of the security control is not applicable to the assessed system per the scoping guidance provided in NIST SP 800-53.

3.4 Phase 4: SCA-Package Preparation

After all security controls have been assessed, the assessor(s) must prepare the SCA-package deliverables using CSO templates for the SCA-report and vulnerability assessment report (VAR).

Figure 6 illustrates each of the steps involved in SCA-package preparation.

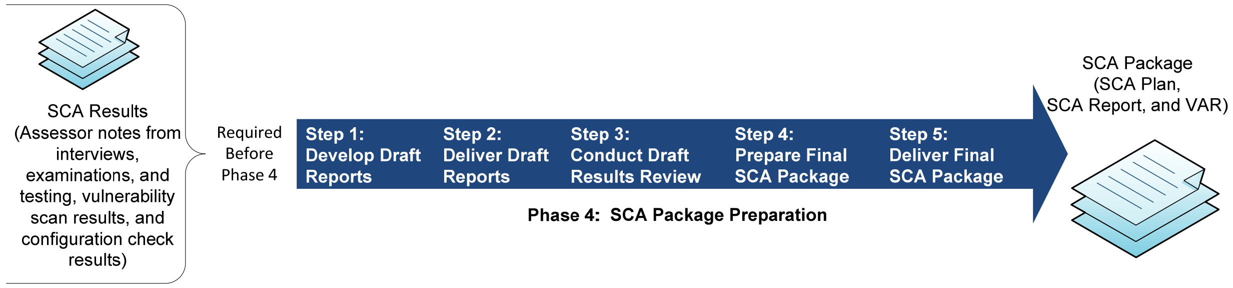

SCA Results
(Assessor notes from interviews, examinations, and testing, vulnerability scan results, and configuration check results)
Required Before Phase 4
Step 1: Develop Draft Reports
Step 2: Deliver Draft Reports
Step 3: Conduct Draft Results Review
Step 4: Prepare Final SCA Package
Step 5: Deliver Final SCA Package
Phase 4: SCA Package Preparation
SCA Package
(SCA Plan,
SCA Report, and VAR)

Figure 6: SCA-Package Preparation

3.4.1 Develop Draft SCA-Report

The assessor(s) must document the preliminary assessment results in a draft SCA-report using the CSO SCA-report template.

3.4.1.1 Assessment Findings

For each assessment objective, the assessor(s) must provide the following:

- A finding (Satisfied, Other than Satisfied, Provided at Agency Level, Provided by <XYZ System>, Risk-based Decision, or Not Applicable) for each assessment objective supported by a determination statement.
- For Satisfied findings, a supporting note that:
  - explains the basis for determining that the assessment objective was satisfied; and
  - cites evidence that supports the finding, and is commensurate with the assurance requirements associated with the evaluated impact level to each supported security objective (confidentiality, integrity, and availability) as documented within the system’s security categorization (see NIST SP 800-53A for more details).
- For Other than Satisfied findings, a supporting note that:
  - explains the basis for determining that the assessment objective was not satisfied;
  - cites evidence that supports the finding; and
  - explains the potential for compromise to confidentiality, integrity, and availability due to the lack of protection associated with the finding;
- For Provided at Agency Level findings, a supporting note that:
  - explains that the assessment objective is completely provided by the NRC at the agency level;
  - cites CSO-STD-0021, “Common and Hybrid Security Control Standard” and the supporting SSP as evidence that the assessment objective is provided by the NRC; or
  - cites CSO-STD-0020 as evidence that a value is defined by the organization.
- For Provided by <XYZ System> findings, a supporting note that:
  - explains that the assessment objective is completely provided by another agency system; and

  - cites a signed, currently effective service level agreement as evidence that the assessment objective is provided by the other system. Systems owned by the same organization are not required to have a service level agreement.
- For Risk-based Decisions findings, a supporting note that:
  - explains that the assessor(s) reviewed the deviation request or waiver request, and approval memos per the requirements in CSO-PROS-1324, “Deviation/Waiver Request Process”;
  - explains that compensating controls and mitigating factors were reviewed and tested and how, that assessor(s) confirmed that the weakness still exists, the driving factor is still relevant, documented mitigating factors and compensating controls are in place, functioning as expected and delivering desired results, the associated risks are evaluated and documented and continue to be consistent with policy and the organization's evolving risk tolerance levels; and
  - cites the deviation request or waiver request and DAA approval memo as evidence that the NRC DAA formally accepted the risk associated with the lack of protection.
- For Not Applicable findings, a supporting note explaining why the assessment objective for the security control is not applicable to the system.

Section 3.3.4 of this process provides criteria for assigning assessment findings. Appendix C of this process provides examples of documented assessment findings.

3.4.1.2 Overall Security Control Status

After assigning assessment findings and providing notes concerning each assessment objective, assessor(s) must review the findings, and then provide a status that communicates the overall effectiveness of each security control. Figure 5 on page 28 of this process provides a decision table to be used as a tool when determining the overall status of each assessed security control (and enhancement), and an example illustrating use of the decision table to determine the overall status of the AC-1 security control.

3.4.1.3 Risk Analysis

The assessor(s) must analyze every security control with an assessment finding of “other than satisfied” or “risk-based decision,” including associated vulnerabilities documented in the VAR, to determine the overall risk to the agency posed by each finding. To make these risk determinations, the assessor(s) must consider, based on current threats, how likely each vulnerability is to be uncovered and exploited by an attacker, and the potential technical and business impact to the system and organization. The business impact shall be considered within the context of the acceptable level of risk established by the organization’s business area leader in addition to the agency’s current risk tolerance if the information is available.

Assessor(s) must recommend strategies for mitigating the potential risk. When recommending mitigation strategies, assessor(s) shall consider:

- the agency’s current risk tolerance;
- the level of risk that is acceptable to the business area leader if the information is available and
- the level of effort, cost, emerging technologies, time constraints, and feasibility of mitigating the risk to an acceptable level.

The SCA-report is provided to the DAA for consideration when making the authorization decision; therefore, the SCA-report must also provide an analysis of the overall risk posed to the agency by operating the system with unmitigated risks. The SCA-report must also clearly identify and point out any significant risks that the assessor(s) believes require mitigation before authorizing the system for operation.

3.4.2 Develop Draft VAR

The assessor(s) must document identified vulnerabilities in a draft VAR using the CSO VAR template. The VAR must provide a summary of the system's strengths and weaknesses, then list all vulnerabilities detected during vulnerability scans and configuration checks of system components. When preparing the VAR, the assessor(s) shall use the data provided in the supporting Findings Tracking Workbook that was created after reviewing and analyzing the raw scan results to remove known false positives and identify any approved deviations or waivers that may apply to the vulnerabilities. Any vulnerabilities that have been verified as remediated, as described in Section 3.3.3.2, shall not be included in the VAR.

Specifically, the following information must be provided for each vulnerability listed in the report:

- the hostname of the affected host;
- the vulnerability ID provided by the scanning tool (e.g., Nessus 20927, DISA-V0001074);
- a description of the vulnerability in language that can be easily understood by non-technical personnel;
- the vulnerability severity level (Critical, High, Moderate) determined by the assessor(s) after considering the severity level assigned by the scanning tool within the context of the system component's environment of operation;

  A risk analysis must also be conducted by the assessor(s) and provided separately in the SAR (delivered with the SCA-report and VAR as part of the SCA-package).

- a recommendation for remediating the vulnerability with sufficient detail such that system personnel can implement the recommendation;
- the NIST SP 800-53 controls affected by the vulnerability; and
- The status of the vulnerability:
  - New POA&M: The vulnerability was discovered for the first time during scanning conducted in support of the assessment.
  - Existing POA&M: The vulnerability was identified during a system scan conducted before the assessment effort, and the status of the vulnerability is already being tracked in the system POA&M.
  - Approved Deviation or Approved Waiver: The vulnerability was identified during a system scan conducted before the assessment effort, and the NRC DAA has accepted the risk associated with the vulnerability via a formal deviation or waiver approval memo. When this is the case, the ADAMS accession number for the memo must also be provided.

After reporting the above for every identified vulnerability, the assessor(s) must provide the total number of vulnerabilities determined by the assessor(s) to be critical, high, moderate, and low severity for each of the scanning tools and configuration specifications used to conduct configuration checks during the assessment.

3.4.3 Deliver Draft SCA-Report and VAR for Review

The assessment project manager or designee must deliver the draft SCA-report and VAR to the system ISSO and CSO representative at least five (5) business days prior to the draft SCA-results meeting.

The draft reports must be delivered in a Portable Document Format (PDF) format to the system ISSO and CSO representative. The draft reports shall be delivered via NRC email.

3.4.4 Conduct the Draft SCA-Results Meeting

The assessment project manager or designee shall schedule a meeting with the full assessment team to take place five (5) business days after submitting the draft SCA-report and VAR. The purpose of the meeting is to brief the team on the draft assessment results, address questions or concerns about the results, and provide a final opportunity to the system ISSO to provide evidence that specific assessment objectives are satisfied.

The system ISSO and CSO representative shall provide feedback on the draft reports via comments in the report PDFs or via email.

Evidence that specific assessment objectives are satisfied must be supplied to the independent assessment team no later than two (2) business days after the draft SCA-results meeting. Evidence provided after that time will not be reflected in the final SCA-package deliverables. The report will not be modified without specific evidence to indicate the report findings are in error.

3.4.5 Prepare Final SCA-Package

The SCA-package is the result of an independent assessment and results are documented as they are found; therefore, the independent assessor shall not change the findings unless there is an error in the package. After receiving the feedback provided by the system ISSO and the CSO representative at the draft SCA-results meeting, the independent assessment team shall consider the feedback and incorporate the feedback into the final SCA-Report and VAR SAR.

Preparation of the final SCA-package shall take no more than fifteen (15) business days. Final SCA-package deliverables are:

- **SCA-Plan.** The final SCA-plan shall include the system inventory sample selected for the assessment.
- **SCA-Report**. The SCA-report shall be finalized per the input received from the system ISSO and CSO representative, and included in the package to support the DAA authorization decision.
- **VAR**. The VAR shall be finalized per the input received from the system ISSO and CSO representative.

3.4.6 Deliver Final SCA-Package

Once the final SCA-package is completed, the independent assessment team shall deliver the final SCA-package to the system ISSO. Each deliverable in the final SCA-package shall be delivered in a Protected PDF format to prevent changes from being made to the assessment results.

The SCA-package must be delivered via NRC email. The system ISSO is responsible for adding the deliverables to ADAMS, and for submitting the SCA-package and any supporting documents to the DAA in the authorization package.

CSO-PROS-2102 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
24-Jul-15	1.0	Initial release	Posting to CSO web page and notification to ISSO forum.	As needed

APPENDIX A COMPONENT SPECIFIC BACKGROUND INFORMATION

In order to determine what security requirements are applicable, and to obtain a complete understanding of the system environment and the function of each component within the system, assessor(s) must obtain specific information concerning the components. The sections below describe the information that assessor(s) must, at a minimum, determine for various system components in order to adequately perform an assessment. This information is typically provided by system personnel (e.g., ISSO and system administrators) and should be contained within system documentation. However, assessor(s) must independently verify the provided information during the course of the assessment.

NRC systems are typically comprised of multiple types of components; therefore, assessor(s) must determine the associated information for each type of component that applies.

A.1 ALL COMPONENTS

The assessor(s) shall determine the following for all system components:

- The location of all required system artifacts (as described in Section 3.1.6), build guides, and other relevant vendor documentation.
- The location of a complete, accurate, and up to date inventory for the system that provides information for all hardware, software, and firmware (including vendor, model, role/function, operating system, version information, etc.).
- The ports, protocols, service, and functions required for the operation of the system, and where this information is documented.
- All interconnected systems or networks (internal or external), what data types are handled by the connections, and how data flows between the systems.
- The logical location of all system components on the system (including virtual components), as well as the hardware devices that virtual components reside on.
- Whether all components are currently supported by the applicable vendor.
- Whether the system has remote access capabilities.
- Whether the system has wireless capabilities.
- What system components employ identification and authentication mechanisms, and where the mechanisms are sourced or operated from, and who they are managed by, especially covering how only authorized identified users obtain access
- What system components employ encryption, what the nature of the encryption is, and whether or not it is FIPS 140-2 validated.
- What system components, if any, are externally facing.
- What system components, if any, are located in non-NRC facilities.

A.2 NETWORK DEVICE COMPONENTS

Network devices are the hardware components used to connect other system components for the purpose of sharing data, resources, or services. To assess a network device properly, an assessor must first understand the function and capabilities of the device. Based on their function, network devices operate at different layers of the Open Systems Interconnection (OSI) model (ISO/IEC 7498-1). For example:

- Repeaters and hubs operate at the physical layer (Layer 1) of the OSI-model; therefore, they are not capable of examining the content (data) carried within the signals that they regenerate and transmit.
- Switches typically operate at the data link layer (Layer 2); therefore, when this is the case, they only examine content supported by layer 2 protocols (e.g., Ethernet, or 802.11 WiFi).
- Routers (and some switches) operating at the transport layer (Layer 3) and examine content supported by layer 3 protocols (e.g., the Address Resolution Protocol [ARP], IPv4, IPv6, and IPSec).

Examples of network devices include, but are not limited to gateways, routers, network bridges, switches, hubs, and repeaters. Multilayer switches, protocol converters, bridge routers, proxy servers, firewalls, network address translators, multiplexers, network interface controllers, wireless network interface controllers, modems, line drivers, and wireless access points are also examples of network devices.

Assessor(s) shall determine the following for assessed network device(s):

- The type of network device (e.g., firewall, router, switch, etc.). This is typically specified for each device in the system inventory.
- The vendor and model.
- The role of each network device, for example:
  - For switches, whether the switch is a Layer 2 or Layer 3 switch.
  - For routers, whether the router is functioning as a boundary protection device.
  - What functional and security options and services are enabled in the device. This includes the devices remote administration and web services it may provide.
- Where network devices are located within the system's network topology. This typically requires a complete and accurate system network diagram that clearly depicts the boundary for the system and any interconnecting systems.
- For boundary protection devices (e.g., firewalls, intrusion detection systems, intrusion prevention systems, etc.):
  - Whether the device is located at an internal boundary or external boundary (including whether intrusion detection/prevention systems are host based or network based).
  - How the device is configured to filter traffic (static packet filtering vs. dynamic packet filtering). This typically involves viewing the configuration file(s) for the device.
  - Whether the device filters traffic using whitelisting or blacklisting.
  - Whether the device performs ingress filtering, egress filtering, or both.

  - Whether the most recent version of firmware is installed on the device (including the latest signatures).
- Whether the network device is approved or has limited approval in the agency Technical Reference Model (available from OIS).
- For network devices used to establish virtual private networks (VPNs):
  - What the connection endpoints for the virtual private network (VPN) are.
  - Where the VPN Gateway is located within the system boundary.
  - The nature of the encryption used by the VPN, whether it is FIPS-140-2 validated, and the tunneling protocol used.
  - How VPN certificates and crypto keys are managed and distributed.

A.3 DATABASE SERVER COMPONENTS

Database servers are typically software components that provide database services to other system components in a client–server relationship. Dedicated hardware components may also be used to provide database services. Examples of database server components include, but are not limited to Microsoft® SQL Server[4], Sybase® Adaptive Server Enterprise (ASE)[5], and Oracle® Hyperion EssBase[6].

Assessor(s) shall determine the following for assessed database server components:

- The vendor and model of each database server.
- The type of database, including the version, running on each database server (e.g., Microsoft SQL 2008 R2, Oracle 10g Release 2, etc.).
- The type(s) of data stored in the database, as identified in the security categorization.
- How encryption is used within the database, including whether all required data is encrypted and whether the database uses FIPS-140-2 validated encryption.
- Where the database resides within the system boundary, externally, or both
- Who has access to the various components of the database, including whether any external users or systems have access to the database, and how the data is accessed.
- How data is input into the system, including whether the database performs input validation for data entries.
- What protocols are used to communicate with the database.
- Whether the database server is approved or has limited approval in the agency Technical Reference Model (available at http://portal.nrc.gov/edo/ois/bpiad/EASB/TRM/default.aspx).

A.4 APPLICATION SOFTWARE COMPONENTS

Per ITIL®, application software is “the software that provides functions that are required by an IT service. Each application may be part of more than one IT Service, and an application runs on

[4] Microsoft is a registered trademark of Microsoft Corporation in the U.S.A. and/or other countries.
[5] Sybase is a registered trademark of Sybase, Inc. in the U.S.A.
[6] Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

one or more servers or clients."[7] At its most basic level, an application is the software that allows a system to provide business functions to the organization. Examples of applications include Microsoft SharePoint, JBoss, IBM WebSphere, and Apache Tomcat. Custom applications are often developed in support of an organization's unique mission and business functions.

Assessor(s) shall determine the following for assessed application software components:

- How users access the application, its interfaces and audience.
- Whether the application consists of custom code, what types (i.e., mobile, web, CGI, etc.) and what the processes are for reviewing, testing, validating, and managing changes to such code. All custom code will be sampled and a code review performed on the sample by the assessor.
- What data flows between different components of the application (e.g., client, server, middleware, etc.) and how. Also the business or mission purpose of each data flow must be identified. This typically requires a complete and accurate data flow diagram that clearly depicts the application components as well as any interconnecting systems.
- What ports, protocols, and services are required for the application, and where the information is documented.
- Whether the application performs input validation for all forms and fields.
- Whether the application is approved or has limited approval in the agency Technical Reference Model (available at http://portal.nrc.gov/edo/ois/bpiad/EASB/TRM/default.aspx).

A.5 WEB BASED COMPONENTS

Web based components include hardware or software used to deliver web content (e.g., websites) that can be accessed through the Internet. The most common use of web servers is to host websites; web applications are often used to run applications from a remote location which users then access with a web browser.

Assessor(s) shall determine the following for system components that contain one or more web server(s):

- The vendor and model of the hardware, including any virtual machine components, running each web server.
- The type of software, including the version, running on each web server (e.g., IIS v6.0, Apache v2.2, etc.).
- Where the web servers reside within the system boundary and on the NRC network (e.g., in the DMZ, etc.).
- Whether the web based system is used internally or has externally facing components, including whether any parts of the system are public facing.
- The type of content the web based system is comprised of, including whether any dynamic or active content is used.
- The type of mobile code (e.g., ActiveX, Flash, etc.) used within the system, if any.

[7] ITIL® V3 Glossary v3.1.24, 11 May 2007

- The types of connections that are used between various components of the web based system.
- The types of certificates or other authentication methods used within the web based system, as well as how the authentication is provided and managed to meet both NIST, OMB, (NIST SP800-63-2) and NRC required eAuthentication specifications.
- Whether the web server is approved or has limited approval in the agency Technical Reference Model (available at: http://portal.nrc.gov/edo/ois/bpiad/EASB/TRM/default.aspx).
- How the web based system interfaces with backend databases or other system components, including the ports and protocols used for this communication, including the authentication method(s) or eAuthentication, as applicable.

A.6 PRIVATE BRANCH EXCHANGE COMPONENTS

Private Branch Exchange (PBX) components are used to support voice and data communications within an enterprise. Components typically used in a PBX include logic cards, switching and control cards, power cards, the PBX's internal switching network, and related devices that facilitate PBX operation.

Vendor personnel are typically the only individuals with administrator access to PBX systems. Since assessing PBX components requires administrator access, assessor(s) must work with the system ISSO to ensure that an individual with administrator privileges is available to assist during the assessment.

Assessor(s) shall determine the following for Private Branch Exchange (PBX) components:

- Whether the PBX system is hosted (delivered by a 3rd party service provider over the Internet), or is supported internally using components installed at the facility.
- The layout of the PBX system and the location of PBX devices within the system. This typically requires a complete and accurate system network diagram that clearly depicts the boundary for the system and any interconnecting systems.
- Whether the system has any Voice over Internet Protocol (VoIP) capabilities, and whether VoIP is used on the system.
- If the system uses VoIP, how the system is segregated from other systems and networks, and who provides and/or manages the VoIP.
- The type of information stored in the system (e.g., voicemails, call records, etc.), including where this information is stored and how the information is protected.
- The type of devices, including any network devices (e.g., firewall, router, switch, etc.) within the PBX system boundary (this typically requires a complete and accurate system inventory and network diagram).
- What ports, protocols, and services are required for the PBX communication, and where this information is documented.
- What ports are used to administer and maintain the PBX, and what safeguards are in place to protect them.
- How voicemail passwords must be configured.

- How extensions and voice mailboxes are handled for terminated employees.
- The level of responsibility, oversight, and control that the PBX vendor has, and whether this is documented in a formal service level agreement and/or vendor maintenance contract.

A.7 VIDEO TELECONFERENCING COMPONENTS

Video teleconferencing (VTC) components are used to provide video teleconferencing services to the agency. VTC hardware components include cameras, microphones, speakers, displays, codex, and the network devices that are used to establish communication between the endpoint devices located at each site that is participating in the conference. VTC software components are also available, and VTC codex may be implemented strictly using software.

Assessor(s) shall determine the following for assessed video conferencing components:

- The type, vendor, and model of each video conferencing hardware component within the system boundary (this is typically specified in the system inventory).
- The location (physical and logical) of all audio/visual devices (this typically requires a complete and accurate system diagram).
- The types of communication that the audio/visual system is primarily used for.
- Where the endpoints of audio/visual communication are located.
- How the audio/visual devices are connected to each other, including the types of connections between endpoints (e.g., dedicated T1 line, etc.)
- Whether the audio/visual traffic uses IP or PSTN.
- Whether the audio/visual system has the capability for remote administration.
- Whether there is a capability to automate certain actions on the system (e.g., scheduling a conference at a certain time automatically activates the microphone and other audio/visual devices at that time).

A.8 SUPERVISORY CONTROL AND DATA ACQUISITION COMPONENTS

Supervisory Control and Data Acquisition (SCADA) components are used to monitor and control the processes and equipment that support facility management systems such as heating, ventilation, and air conditioning (HVAC) systems, lighting systems, and security systems. Examples of SCADA components include, but are not limited to sensors, control relays, remote telemetry units (RTU’s), master units, and the network devices that are used to establish a connection between the master unit and each of the RTU’s.

Assessor(s) shall determine the following for assessed SCADA components:

- The nature of the industrial or facility processes being controlled by the SCADA system (e.g., power generation, physical access control, water treatment, etc.)
- The nature of the software (including operating system) used to control the SCADA system.
- The type, vendor, and model of SCADA within the system boundary (this is typically specified in the system inventory).

- The location (physical and logical) of all SCADA devices and equipment (this typically requires a complete and accurate system diagram).
- Whether the SCADA system interconnects with any other network or system.

APPENDIX B REQUIRED ASSESSMENT PROCEDURES

This appendix provides the procedures that assessors must use to assess each security control in a system's security control baseline. The procedures must be performed for every applicable component of the system within the CSO approved sample selected for assessment. For example, if more than one system component within the sample contains unique user accounts (e.g., operating system accounts, application accounts, database accounts, etc.), all account management assessment procedures must be performed for each type of account. If the assessor(s) identify a finding for any component or any account of the system, then they must indicate that the AC-2 control is Other than Satisfied (deficient) and assign a severity level to the deficient control.

Assessment objects shall be evaluated based on currently effective cybersecurity guidance and the NRC defined values within CSO-STD-0020. NIST SP 800-53 provides supplemental guidance for all security controls and may be used as a reference regarding proper security control implementation.

B.1 REQUIRED RIGOR AND SCOPE

The rigor and scope applied to each procedure must be sufficient to demonstrate that the assurance requirements associated with the assessed security control have been satisfied, or to support assessor findings that indicate that the requirements have not been satisfied.

Per NIST SP 800-53A, "the rigor and scope of the assessment increases in direct relationship to the assurance requirements." The assurance requirements for assessed systems increase in relationship to the potential security risk impact (high, moderate, or low) to an organization (and its resources, users, partners etc.) if events were to occur that jeopardized the security objectives for the system and/or the information processed and stored on the system. Therefore, the rigor and scope applied to each assessment procedure must be based on the highest evaluated impact level to each of the applicable security objectives (confidentiality, integrity, and availability) as documented within the system Security Categorization.

For example, when assessing the SC-7, Boundary Protection control for a system evaluated to have a high impact level to confidentiality; assessors must conduct comprehensive tests of boundary protection hardware and software and review a significant number of supporting system artifacts (e.g., procedures addressing boundary protection; system configuration settings and associated documentation; or records of exceptions to traffic flow policies). The goal of the assessment is to provide a high degree of confidence that the organization has effectively implemented security controls to protect the confidentiality and integrity of the information being transmitted by the system, and to provide strong evidence in support of the assessment finding.

B.2 ACCESS CONTROL (AC)

Access control assessment objects include, but are not limited to: access control policy and procedures; account management documentation; account settings (as displayed on the account management console); records of account reviews; configuration settings for automated access control mechanisms; and tasks performed by staff personnel in support of access control functions.

B.2.1 AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Interview

Are system-specific access control policies and procedures available?

Who is responsible for reviewing, updating, and disseminating these procedures?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.

Review the system policy to determine whether it aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated access control controls.

Examine records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to.

Examine records to determine whether or not policy and procedures were disseminated to the organization elements.

Review the system-specific access control policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO PROC 2104, “System Artifact Examination Procedure.”

B.2.2 AC-2 ACCOUNT MANAGEMENT

Interview

What is the process for granting a user access to the system? Please describe all steps from the initial request to user access (e.g., request, approval, implementation, and notification that access is granted).

Who manages system accounts? If it is more than one role/individual, where is the separation of duties between these individuals?

Who reviews the system accounts?

How often are the system accounts reviewed?

What are the account types for the system (i.e., individual, group, and system)?

What types of groups are applicable in the system? (e.g., Administrators, Users)

What are the conditions for group membership?

How are associated authorizations assigned?

Is access role based, or are specific rights granted on a per individual basis? If granted on a per individual basis, then how are assigned authorizations granted (criteria)?

How are account managers notified when users are terminated, transferred, or there is a change in need to know/need to share status?

What is the process for removing, disabling, or otherwise securing these accounts in such cases?

Examine

Review relevant system documentation addressing account management to determine whether the types of system accounts used by the system and the measures used to manage the accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts are identified, and to obtain an understanding of the organization's approach to account management.

Examine a sample of user accounts in the account management console to determine whether account groups and roles are implemented as described in system documentation.

Examine account management records to determine whether there is evidence demonstrating that accounts were disabled or removed entirely for recently transferred, separated, or terminated employees.

Observe authorized system personnel as they create, enable, modify, disable, and remove accounts per NRC defined requirements.

Examine records of account reviews to determine whether system accounts have been reviewed per NRC defined requirements.

Enhancement 1

Interview

Does your organization use an automated mechanism to assist with account management?

Examine

Review relevant system documentation addressing account management to determine whether the organization uses automated mechanisms to support account management functions, and, if so, how the mechanisms are configured.

Observe authorized system personnel as they use the automated mechanisms, and determine whether the mechanisms function as described in the system documentation.

Test

Arrange with the system ISSO and system administrator staff to login to and demonstrate the automated mechanisms used to assist with account management. Observe the use of their functions under test or live use conditions and ensure that they function as described in system documentation.

Enhancement 2

Interview

Does the mechanism automatically remove/disable temporary and emergency accounts? How frequently are they removed or disabled?

Examine

Review the configurations of automated account management mechanisms to ensure that they automatically remove/disable temporary and emergency accounts in accordance with NRC defined timeframes, and to obtain an understanding of the organization's approach to account termination.

Test

Using an approved test sequence and approach, access and exercise the system's account management functions to determine whether the organization terminates all temporary and emergency accounts after the NRC required timeframe.

Inspect automated account management mechanisms to determine whether they in fact automatically remove/disable temporary and emergency accounts after the NRC required timeframes.

Enhancement 3

Interview

Does the mechanism automatically disable inactive accounts? How frequently are they disabled?

Examine

Review relevant system documentation addressing account management to determine whether the organization uses account management mechanisms to automatically disable inactive accounts after the NRC required timeframe, and to obtain an understanding of the organization's approach.

Test

Review the configurations of automated account management mechanisms to ensure that they automatically disable inactive accounts in accordance with NRC defined timeframes.

Enhancement 4

Interview

Does the mechanism automatically audit account creation, modification, enabling, disabling, and removal actions? Who is notified when these events occur?

Examine

Review relevant system documentation addressing account management to determine whether the organization uses automated account management mechanisms to audit account creation, modification, disabling, and termination, and to obtain an understanding of the organization’s approach.

Test

Work with the system ISSO and system administrator team as required to run the automated account management mechanisms through some test steps observing the procedures taking place and then inspecting audit logs to ensure that they automatically audit account creation, modification, enabling, disabling, and removal actions and notify NRC defined personnel.

Enhancement 5

Interview

Does your organization require that users log out after a specific time period or whenever specific events occur? What is the time period? What are the events?

Examine

Review relevant system documentation addressing account management to determine whether the organization uses automated mechanisms to automatically log users out in NRC defined circumstances, and to obtain an understanding of the organization’s approach.

Test

Working with the system ISSO and/or system administrator team, perform account use exercises designed to check if the automated account management mechanisms do in fact automatically log users out in accordance with NRC defined circumstances. Witness and document the results.

Enhancement 11

Interview

Does your organization have documented usage conditions for system accounts? Are they enforced and if so, how are they enforced?

Examine

Review relevant system documentation addressing account management to determine whether the organization uses automated mechanisms to enforce usage conditions, to determine who is notified, and to obtain an understanding of the organization’s approach.

Inspect automated account management mechanisms to determine whether they are configured to monitor accounts for usage conditions, and to determine who is notified if usage condition violation is detected.

Enhancement 12

Interview

Does your organization monitor the system for atypical usage of accounts? Who does your organization report atypical use to?

Examine

Review relevant system documentation addressing account management to determine whether the organization uses automated mechanisms to monitor the system for atypical usage of accounts, to determine who is notified, and to obtain an understanding of the organization's approach.

Inspect automated account management mechanisms to determine whether they are configured to monitor for atypical usage of accounts, and to determine who is notified if atypical usage is detected.

Enhancement 13

Interview

If you are aware that an individual poses a risk to the NRC or your organization, how long does it take you to disable their account(s)?

Examine

Review relevant system documentation addressing account management to determine whether the organization uses automated mechanisms to disable accounts of users who pose a significant risk within NRC required timeframes, and to obtain an understanding of the organization's approach.

Inspect automated account management mechanisms to determine whether they are configured to disable the accounts of users who pose a significant risk within NRC required timeframes.

B.2.3 AC-3 ACCESS ENFORCEMENT

Interview

How is logical access to information and system resources enforced?

What types of access enforcement mechanisms does the system employ that control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the system?

Are access enforcement mechanisms employed at the application level, when necessary, to provide increased information security?

What are the steps to override automated mechanisms (if any) in the event of emergencies or other serious events? In what way are these steps or procedures controlled, audited, or manually overridden?

Were access control policies defined in the development phase?

Does the COTS documentation outline the access control policies?

Examine

Review relevant system documentation addressing access enforcement to determine whether the organization uses mechanisms to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies, and to obtain an understanding of the organization’s approach to access enforcement.

Test

Observe a sample of access enforcement mechanisms to ensure that account groups and roles are implemented as described in system documentation, including the associated permissions of each group or role.

If possible, observe a user with non-privileged access authorizations log onto the system and ensure that their access to the system is limited as expected.

Observe the test steps performed to override (or attempt to override) automated mechanisms (if any) in the event of emergencies or other serious events to ensure the control functions operate as intended.

If the system encrypts stored information as a means of access enforcement, inspect the properties and effectiveness of the encryption mechanism(s) to ensure it is FIPS-140-2 validated, and the intended files, folders, records and/or content is properly encrypted.

B.2.4 AC-4 INFORMATION FLOW ENFORCEMENT

Interview

How does the system enforce approved authorizations for controlling the flow of information within the system and between interconnected systems?

Does the system enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy?

What are source and destination flows within the system?

What are source and destination flows outside the system?

What are the information characteristics of data traversing these flows/paths? Can it be traced to FIPS-199?

What internal boundary protection mechanisms or devices reside within the system (intra system communication)?

What external boundary protection mechanisms or devices reside outside the system?

Examine

Review relevant system documentation addressing information flow enforcement to obtain an understanding of the organization’s approach.

Review the configurations of internal and external boundary devices within the system (e.g., firewalls, proxy servers, etc.), as well as any other devices that control information flow within the system (routers, switches, etc.), to ensure the organization may control the flow of information within the system and between interconnected systems as described by system documentation and in accordance with NRC defined requirements.

Test

Observe the actual use and/or operation of the management consoles of internal and external boundary devices within the system, as well as any other devices that control information flow within the system, to ensure that the system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with NRC defined requirements.

B.2.5 AC-5 SEPARATION OF DUTIES

Interview

How does your organization enforce separation of duties? Does the system enforce separation of duties through assigned access authorizations?

Is there access control software on the system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion?

What features or functions of the software prevent users from having all the necessary authority or access privileges to perform fraudulent activity?

What are the roles that should be separated?

Does the system have a roles and responsibilities document?

Are divisions of responsibility designated so as to eliminate conflicts of interest?

Are there any conflicts of interest or excessive access rights or privileges in the system based on how responsibilities are currently designated?

Are there appropriate safeguards to enforce appropriate levels of need-to-know based access and only the level of access required to perform authorized job duties?

Examine

Review relevant system documentation addressing the division of responsibilities and separation of duties to determine whether the organization identifies the separation required to eliminate conflicts of interest.

Review relevant system documentation addressing separation of duties to determine whether the organization uses mechanisms to enforce separation of duties, and to obtain an understanding of how they are used.

Test

Observe actual use and operation (or test use) of the system's access enforcement mechanisms or other applicable software features or functions to ensure that separation of duties is enforced as described in system documentation and in accordance with NRC defined requirements. For example, privileged security functions, settings, or info should not be accessible or useful to non-privileged accounts.

B.2.6 AC-6 LEAST PRIVILEGE

Interview

How does your organization enforce the concept of least privilege?

Are there system components, functions, or tasks that require more restrictive access requirements due to increased risk to the system?

Are these tasks administered by users or system processes running on behalf of a user?

What are the enforcement mechanisms?

Examine

Review relevant system documentation addressing the concept of least privilege to determine whether the organization grants limited rights/privileges or access to users to enable performance of specified tasks while adequately mitigating risk to the organization, individuals, other organizations, and the Nation.

Test

Working with the system ISSO and system administrator staff attempt different test use scenarios to check and ensure if enforcement mechanisms or other applicable software features or functions enforce least privilege access as described in system documentation and in accordance with NRC defined requirements.

Enhancement 1

Interview

What security functions and security relevant information have been defined by the project as requiring explicit authorization for access?

Examine

Review relevant system documentation addressing access enforcement to determine which system functions and information require explicit authorization for access.

Review relevant system documentation addressing access enforcement to determine whether the organization explicitly authorizes access to the organization defined security functions and security relevant information.

Test

Perform test events against a sample of the mechanisms, software features, or functions to determine whether the system enforces any organization defined explicitly authorized access requirements to the system’s security functions and security relevant information. Witness the system’s response to ensure that access is in-fact limited to only those users granted that authorization.

Enhancement 2

Interview

Do users with privileged accounts use non-privileged accounts or roles, when accessing non-security functions? Please provide an example.

Examine

Review relevant system documentation addressing access enforcement functions to determine whether users with privileged accounts use non-privileged accounts or roles when accessing non-security functions.

Test

Observe the non-privileged accounts or roles used by users with privileged access when performing non-privileged types of tasks and duties.

Enhancement 3

Interview

When are privileged users authorized to access the system via a network connection (as opposed to locally)? What are they authorized to do? Is the rationale for this documented in your SSP?

Examine

Review relevant system documentation addressing access enforcement functions to determine whether network access is only authorized for NRC defined privileged commands.

Test

Working with the system ISSO and system administrator staff perform functional level security checks against the system's access enforcement mechanisms. During the testing observe a sample of access enforcement mechanisms or other applicable software features or functions to ensure that network access is only authorized for NRC defined privileged commands.

Enhancement 5

Interview

Who are privileged accounts provided to (please provide roles or personnel)?

What system components provide privileged accounts?

What system functionality do privileged accounts provide access to?

Examine

Review relevant system documentation addressing privileged accounts to determine which system components contain privileged accounts.

Review relevant system documentation addressing privileged accounts to determine whether they are restricted to personnel as described in system documentation and in accordance with NRC defined requirements.

Test

Working with the system ISSO and system administrator team make and observe attempts to access or use privileged accounts on the system to ensure that they are restricted to personnel as described in system documentation and in accordance with NRC defined requirements.

Enhancement 9

Interview

Does the system audit the execution of privileged functions?

Examine

Review relevant system documentation addressing auditing of privileged accounts to determine whether the system audits the execution of privileged functions, such as account management actions.

Review audit logs to determine whether the system audits the execution of privileged functions, such as account management actions.

Test

Work with the system ISSO and system administrator staff to carry out some test use of selected privileged functions on the system. Locate and review a sample of applicable audit logs for those transactions for that time period to ensure that the system audits the execution of privileged functions, such as account management actions.

Enhancement 10

Interview

Does the system prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures?

Examine

Review relevant system documentation to determine whether the system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Test

Observe a sample of access enforcement mechanisms or other applicable software features or functions to ensure that non-privileged users are unable to execute privileged functions.

Work with the system ISSO and system administrator team to arrange for and observe a user with non-privileged access authorizations log onto the system and ensure that their access to the system is limited as expected.

B.2.7 AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Examine

Review relevant system documentation to determine whether the organization uses mechanisms to enforce the limit of consecutive invalid logon attempts and to obtain an understanding of the organization’s approach to access enforcement.

Review the configurations of automated account management mechanisms to ensure that the system enforces the NRC defined limit of invalid access attempts.

Test

Working with the system ISSO and system administrator staff and with a sample of user accounts, execute testing steps within the system to determine if the automated account management mechanisms ensure the system enforces the NRC defined action(s) for the NRC defined length of time once the unsuccessful logon threshold has been reached.

B.2.8 AC-8 SYSTEM USE NOTIFICATION

Examine

Review relevant system documentation to determine whether the organization uses automated mechanisms to display a system use notification message (banner) before granting system access.

Test

Observe a user log onto the system and ensure that the system displays the NRC defined system use notification message prior to granting access to the system, and that the system retains the notification message on the screen until the user takes explicit actions to log on to or further access the system.

B.2.9 AC-10 CONCURRENT SESSION CONTROL

Examine

Review relevant system documentation to determine whether the organization uses automated mechanisms to limit the number of concurrent user sessions and to obtain an understanding of the organization’s approach to concurrent session control.

Review the configurations of automated account management mechanisms to ensure that the system may enforce the NRC defined limit concurrent sessions.

Test

Observe a user logging onto the system. Arrange for the user to attempt multiple user sessions (and extra sessions) to determine whether the number of concurrent sessions is limited to the NRC permitted number of concurrent sessions.

B.2.10 AC-11 SESSION LOCK

Examine

Review relevant system documentation to:

- Obtain an understanding of the organization’s approach to session locks.
- Determine whether the organization uses automated mechanisms to initiate session locks after the NRC defined period of inactivity.
- Determine whether system components permit users to directly initiate session lock mechanisms.

Review the configurations of automated account management mechanisms to ensure that the system may enforce the NRC defined period of inactivity before initiating a session lock.

Review the configurations of automated account management mechanisms to ensure that the system may prevent further access to the system after initiating a session lock, and that the session lock should remain in effect until the user reestablishes access using appropriate identification and authentication procedures.

Test

Observe system users as they attempt to access a locked session without applying organization defined identification and authentication procedures.

Enhancement 1

Examine

Review relevant system documentation to determine whether the system conceals the data on the screen, uses a session lock mechanism, or displays a publicly viewable image.

Test

Work with the system ISSO and/or system administrator to initiate a lock on a sampling of user accounts. Observe a user account with a session lock initiated and ensure that information previously visible on the display is now concealed with a publicly viewable image.

B.2.11 AC-12 SESSION TERMINATION

Examine

Review relevant system documentation to obtain an understanding of the organization’s approach to session termination, and to determine whether the organization uses automated mechanisms to terminate remote sessions.

Test

Work with the system ISSO and system administrator using a sampling of system user accounts to exercise the conditions that should disconnect a user session. Observe the operation of the automated account management mechanisms to ensure the system automatically terminates a user session after the NRC defined conditions requiring session disconnect.

B.2.12 AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Interview

What user actions can be performed on the system without identification and authentication?

Where are these actions documented?

Do these actions pertain to public facing components of the system only?

Examine

Review relevant system documentation to obtain an understanding of the specific user actions (if any), that the organization permits to be performed on the system without identification or authentication.

Test

Work with the system ISSO and system administrator staff to attempt actions on the system without use of the usual identification and authentication. Observe a sample of actions that can be performed on the system without identification and authentication (if any) to ensure that they operate as described in system documentation.

B.2.13 AC-17 REMOTE ACCESS

Interview

Does the organization allow remote access for components other than public web servers or components specifically designed for public access?

What types of remote access are in place or planned on the system?

Who authorized the use of and types of remote access for the system?

How does the organization monitor remote access into the system?

Who is responsible for monitoring remote access on an ongoing basis?

How does the organization restrict remote access and protect against unauthorized connections or subversions of authorized connections?

Are IPsec based VPNs used by the systems for remote access?

Examine

Review relevant system documentation for (1) the list of authorized methods of remote access to include both establishment of the remote connection and subsequent user actions across that connection, and (2) the measures and their configuration settings (where applicable) to be employed to authorize, monitor, and control these implemented methods of remote access to the system.

Test

Working with the ISSO arrange to attempt test instances of unwanted access and witness whether the system monitors for and identifies the attempted remote connections, Observe the remote access management console to ensure that the organization monitors for unauthorized remote access to the system,

Observe a new remote connection get established to ensure that the system requires identification and authentication prior to connection.

Working with the ISSO attempt to make connections using settings or configurations that do not meet the intended requirements, such as weaker encryption, etc.

Observe the remote access management console to ensure that the organization enforces requirements for remote access to the system.

If the system uses federal Personal Identity Verification (PIV) credentials as identification tokens, observe the remote access management console to ensure that the system complies with FIPS-201 and NIST SP 800-73, and 800-78.

Enhancement 1

Interview

Does your organization monitor for unauthorized remote access to the system?

Examine

Review relevant system documentation to:

- Obtain an understanding of the organization’s approach to monitoring and control of remote access methods, and
- Determine whether the organization uses automated mechanisms to facilitate monitoring and control of remote access.

Test

Observe automated remote access mechanisms to ensure that the organization monitors and controls all remote access to the system.

Enhancement 2

Interview

What cryptography is in place to protect remote access sessions (for each remote access method)?

Examine

Review relevant system documentation to

- Obtain an understanding of the organization’s approach to protecting the confidentiality and integrity of remote access sessions.
- Determine whether the organization uses mechanisms that employ cryptography to protect the confidentiality and integrity of remote access sessions.

Test

Observe the properties and status of some sample live automated remote access mechanisms to ensure that all encryption used for remote access is FIPS-140-2 validated.

Enhancement 3

Interview

How many remote access control points does the system employ?

What is the ratio of remote accesses to remote access control points?

How are remote access control points managed? Who manages them?

Examine

Review relevant system documentation to determine whether the organization identifies managed access control points for remote access to the system.

Test

Observe automated remote access mechanisms to ensure that the system routes all remote accesses through managed access control points.

Enhancement 4

Interview

What privileged functions are authorized via remote access? Who in the organization made this authorization?

What are the compelling operational needs for having these functions in use via remote access?

Examine

Review relevant system documentation addressing remote access to privileged functions of the system to determine whether the organization identifies specific situations and compelling operational needs that require remote access to privileged functions on the system.

B.2.14 AC-18 WIRELESS ACCESS

Interview

Does your system have wireless capabilities? Does your organization explicitly authorize wireless access before permitting connections? Are usage restrictions, configuration/connection requirements, and implementation guidance available?

Does the system employ wireless capability or technologies? If so, what are they?

Are usage restrictions defined, and if so, where and by whom?

Is implementation guidance defined, and if so, where and by whom?

Who authorizes wireless access to the system? What is the process?

Who monitors wireless access to the system? What processes and/or procedures are followed?

What controls are in place to restrict/manage wireless access to the system?

Who implements wireless intrusion detection and prevention and how?

Examine

Review relevant system documentation addressing wireless implementation and usage (including restrictions) to:

- Determine if the system provides wireless access, and, if so, whether the organization provides documented wireless usage restrictions and implementation guidance.
- Determine if the organization specifies the measures to be employed to authorize, monitor, and control the use of wireless access.

Test

Observe wireless capabilities or other applicable features or functions on the system, such as intrusion detection software, to ensure that the organization monitors for unauthorized wireless access to the system.

Arrange to attempt both authorized and unauthorized wireless connections to the system. Observe and inspect the wireless capabilities on the system to ensure that the organization explicitly authorizes wireless access before permitting connections. Inspect the wireless access point or systems connection logs ensuring both successful as well as rejected connection attempts are properly logged per CSO standards.

While observing active and attempted sessions determine if wireless capabilities on the system ensure that the organization enforces requirements for wireless access.

Enhancement 1

Interview

What authentication mechanisms are in place to protect wireless access to the system?

Is encryption used to protect wireless access to the system?

Examine

Review relevant system documentation addressing wireless implementation and usage (including restrictions) to obtain an understanding of the mechanisms used for authentication and encryption for the purpose of protecting wireless access.

Test

Observe a new wireless connection get established to ensure that the system implements authentication mechanisms to protect wireless access to the system.

Observe wireless capabilities and monitor/inspect the connection properties in use on the system to ensure that the system implements encryption to protect wireless access, and that encryption mechanisms used are in fact FIPS-140-2 validated.

Enhancement 4

Interview

Who is authorized to configure wireless networking capabilities?

Examine

Review relevant system documentation addressing wireless implementation to determine whether the organization prevents users from independently configuring wireless networking capabilities.

Test

Arrange for and observe attempts by users of different types to make changes to the wireless capabilities on the system. Ensure that any users the system allows to independently configure wireless networking capabilities are only those the organization has explicitly identified as being granted privileges to do so. Witness that any attempts by other users to reconfigure the wireless capabilities fail.

Enhancement 5

Interview

Are radio antennas selected, and are transmission power levels calibrated to reduce the probability that usable signals can be received outside of organization controlled boundaries?

Examine

Review relevant system documentation addressing wireless implementation to determine whether the organization confines wireless communications to organization controlled boundaries.

Test

Using CSO approved Wi-Fi / wireless scanning tools and configurations, do Wi-Fi signal access distance checks (i.e., “war-driving” or walk testing) for NRC network access outside and around the NRC facility in question. Observe wireless capabilities on the system to ensure the organization positions wireless hardware and calibrates transmission power levels to reduce the probability that usable NRC Wi-Fi or wireless signals can be received outside of organization controlled and NRC intended access boundaries. Testing should assess where NRC Wi-Fi networks should be discoverable or accessible and where they should not be.

B.2.15 AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Interview

Are there any organizationally controlled portable or mobile devices? If so, what are the usage restrictions? Where are they defined?

Who authorizes portable or mobile device access to the system?

Who monitors portable or mobile device access to the system?

What controls are in place to restrict/manage portable or mobile device access to the system?

Examine

Review relevant system documentation addressing access control for portable and mobile devices to determine whether the organization has documented the measures and configuration settings to be employed to authorize, monitor, and control device access to organizational systems in accordance with the usage restrictions and implementation guidance.

Test

Using CSO approved Wi-Fi / wireless scanning tools and configurations attempt authorized and unauthorized / incorrect connection types. Observe applicable software features or functions on the system to ensure that the organization monitors for unauthorized access by mobile devices to the system and enforces requirements for the connection of mobile devices to the system. Any connection attempt not meeting all the requirements should be rejected by the system.

Enhancement 5

Interview

What mechanisms are in place to protect the confidentiality and integrity of information on mobile devices?

Examine

Review relevant system documentation addressing access control for portable and mobile devices to determine whether the organization protects the confidentiality and integrity of information on NRC defined mobile devices.

Test

Observe and inspect the properties of a sample of mobile devices approved for use and in use with the system to ensure the devices implement encryption in accordance with NRC defined requirements and that the encryption mechanisms are FIPS-140-2 validated.

B.2.16 AC-20 USE OF EXTERNAL SYSTEMS

Interview

Does the system allow access to/from any external systems? If so, who owns the external system?

What is the system used for?

Are there any agreements in place concerning the application of required security controls?

Are the external system’s security controls assessed for effectiveness?

What information is transmitted to, processed, and/or stored on these external systems?

Examine

Review relevant system documentation addressing the use of external systems (e.g., Memorandum of Understanding, Interconnection Security Agreement, etc.) to obtain an understanding of the organization's terms and conditions for allowing authorized individuals to access the system from external systems.

Enhancement 1

Examine

Review relevant system documentation addressing the use of external systems to determine whether required security controls are implemented on the external system as specified in the organization's information security policy and security plan.

Review approved system connection or processing agreements with the organizational entity hosting the external system to obtain an understanding of the nature and terms of the connection.

Enhancement 2

Examine

Review relevant system documentation addressing the use of external systems to determine whether the organization limits or prohibits the use of organization controlled portable storage devices in external systems.

B.2.17 AC-21 COLLABORATION AND INFORMATION SHARING

Interview

Are authorized users enabled to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information?

Are mechanisms available to assist authorized users in making information sharing decisions?

Examine

Review relevant system documentation addressing the use of collaboration and information sharing to:

- Obtain an understanding of the mechanisms and configuration settings employed to facilitate information sharing decisions, and
- Determine whether mechanisms are implemented in accordance with NRC defined requirements.

Test

Observe mechanisms used to assist authorized users in making information sharing decisions to ensure that they are implemented in accordance with NRC defined requirements. Determine if the information and guidance provided to users when making info sharing decisions is adequate to help guide users in sharing the data with only authorized entities, holding an appropriate clearance level and need-to-know.

B.2.18 AC-22 PUBLICLY ACCESSIBLE CONTENT

Interview

Is system information publicly accessible?

What is the nature of the information?

Examine

Review relevant system documentation addressing publicly accessible content to obtain an understanding of the mechanisms and configuration settings employed by the organization to protect nonpublic information from publicly accessible information.

B.3 AWARENESS AND TRAINING (AT)

Awareness and training assessment objects include, but are not limited to: policy and procedures; training documentation; records of training; and tasks performed by staff personnel in support of awareness and training functions.

B.3.1 AT-1 AWARENESS AND TRAINING POLICY AND PROCEDURES

Interview

Are system-specific awareness and training procedures available?

Who is responsible for reviewing, updating, and disseminating these procedures?

Are there records to support that these reviews and updates took place?

Systems with non NRC users: Are system-specific security awareness and training policies and procedures available? Who is responsible for reviewing, updating, and disseminating the policy and procedures?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether it aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated awareness and training controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to.

Examine records to determine whether or not policy and procedures were disseminated to the organization elements.

Review the system-specific awareness and training policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.3.2 AT-2 SECURITY AWARENESS TRAINING

Interview

Are new users required to take the cybersecurity awareness training within a certain time period of being granted any access to an agency system that requires authenticated access?

Is agency-wide refresher cybersecurity awareness training required? How often? Where is this requirement documented? How is it provided?

Examine

Review relevant system documentation addressing security awareness and training to obtain an understanding of the requirements for cybersecurity awareness training and for formally documenting the both initial and refresher awareness training completion.

Examine the training records of personnel and contractors to determine whether the organization provides security awareness training as an initial user and at the subsequent required frequency.

Select and Interview or survey a sampling of staff members who have completed the training. Ask a few security awareness questions (based on the training) anonymously. The goal is to sample and measure effectiveness of the training, measuring actual staff response based on that training. Document the results. An additional option is to observe actual staff performance with respect to using the training during tasks.

Enhancement 2

Examine

Review the cybersecurity awareness course and determine if the course contains training on and reporting potential indicators of insider threat.

B.3.3 AT-3 SECURITY TRAINING

Interview

Has your organization identified staff with significant IT security roles? If so, where is this documented?

Does your organization provide system-specific vendor/commercial training to your staff with significant IT security roles? If so, how often?

Are there records to support that training occurred?

Does your organization ensure that staff takes CSO provided roles based security courses before being authorized to access the system or performing assigned duties?

Examine

Review relevant system documentation addressing security awareness and training to obtain an understanding of the organization's process for identifying personnel with significant system security roles and responsibilities and for formally documenting the roles and responsibilities for identified personnel.

Examine the training records of personnel identified with system security roles and responsibilities to determine whether the organization provides security training before authorizing access to the system or performing assigned duties and when required by system changes.

Select and Interview or survey a sampling of staff members who have completed the training. Ask a few security awareness questions (based on the training) anonymously. The goal is to sample and measure effectiveness of the training, measuring actual staff response based on that training. Document the results. An additional option is to observe actual staff performance with respect to using the training during tasks.

B.3.4 AT-4 SECURITY TRAINING RECORDS

Interview

Does your organization notify CSO of all system-specific vendor/commercial training attended by staff with significant IT security roles?

Examine

Examine security training records and training activity monitoring artifacts (for example, sign in sheets and training certificates) to determine whether the organization is monitoring and documenting security awareness training and information specific security training.

Interview a selection of staff members and survey them with a few questions regarding what training they believe they completed (they might have certificates or credits for) during the period in review. Compare info with training the organization documented.

B.4 AUDIT AND ACCOUNTABILITY (AU)

Audit and accountability assessment objects include, but are not limited to: policy and procedures; audit logs; audit records; automated auditing mechanisms; and tasks performed by staff personnel in support of audit and accountability functions.

B.4.1 AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Interview

Are system-specific audit and accountability policies and procedures available?

Who is responsible for reviewing, updating, and disseminating these procedures?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated audit and accountability controls.

Examine records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to.

Examine organization records to determine whether or not policy and procedures were disseminated to the organization elements.

Review the system-specific audit and accountability policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, "System Artifact Examination Procedure."

B.4.2 AU-2 AUDITABLE EVENTS

Interview

Which system component(s) carry out auditing activities for the system?

Are all of the auditable events captured by the above component(s)?

Are any additional auditable events captured?

Are events audited on a continuous basis or in response to specific situations? Was this decision based on an assessment of risk? If so, is it documented?

Do any other organizations need audit related information? If so, were they consulted concerning the selection of auditable events?

How often does your organization review auditable events to ensure they are still sufficient?

Examine

Review relevant system documentation to:

- Determine whether auditable events are documented for the system.
- Determine whether the events comply with the NRC required events in CSO-STD-0020.
- Determine whether rationale is provided to support that the auditable events are adequate for after the fact (forensic) security incident analysis purposes.
- Obtain an understanding of the automated mechanisms employed by the organization to generate audit records (into a log file) in accordance with the auditable events.

Test

Review the configurations of audit capabilities on the system to ensure that the system is capable of auditing the NRC defined events.

Enhancement 3

Interview

How often are audit logs reviewed? During the review, are other organizations that need audit related information consulted?

Examine

Review relevant system documentation to determine whether the organization reviews and updates audited events at the NRC required frequency stated in CSO-STD-0020.

B.4.3 AU-3 CONTENT OF AUDIT RECORDS

Examine

Review audit records generated by the system to determine whether the records establish the type of events that occurred, when the events occurred, where the events occurred, the source of the events, the outcome of the events, and the identity of any individuals or subjects associated with the events.

Test

Observe a series of test or live transactions being entered through each interface type. Note the details of those transactions. Examine system logs to ensure that the system generates audit records that capture the required information for the events or transactions submitted.

Enhancement 1

Interview

Can the auditing component(s) be modified to capture additional information that would provide more detailed audit records for events identified by type, location, or subject?

Examine

Review audit records generated by the system to determine whether additional, NRC defined information as defined in CSO-STD-0020 is captured in the records.

Test

Observe transactions or events being entered into the system. Note the details of these events. Observe the operation of the audit capabilities on the system to ensure that the additional, NRC defined information as defined in CSO-STD-0020 is captured in records generated by the system.

Enhancement 2

Interview

Does the system have a centralized software/component for managing the content of system audit records?

Examine

Review relevant system documentation to:

- Determine whether the organization uses automated mechanisms to centrally manage the content captured in audit records, and
- Obtain an understanding of the mechanisms and how they are configured to provide a centralized management capability for the content of audit records generated from multiple components throughout the system.

Test

Work with the ISSO and system administrator to demonstrate this centralized software component. Observe use of the audit management console on the system to ensure that the system implements a centralized software/component for managing the content of system audit records.

B.4.4 AU-4 AUDIT STORAGE CAPACITY

Interview

How much storage capacity has been allocated to audit records?

What percentage of the allocated storage is currently being utilized?

Has the storage ever been exceeded? If so what happened?

What are the system configuration settings that will reduce the likelihood of the audit record storage capacity being exceeded?

When capacity is reached, where are the records stored? Does the organization have a process for off-loading the records to an alternate system or storage media? Is the process documented?

Examine

Review relevant system documentation to:

- Determine the audit storage capacity to be allocated for the system, and
- Determine whether the organization provides adequate rationale that the capacity is sufficient to accommodate typical auditing and audit processing requirements, and to reduce the likelihood of audit record storage capacity being exceeded is provided.

Test

Work with the ISSO and system administrator to observe the audit management console used on the system to ensure that the system allocates audit record storage capacity in accordance with NRC defined requirements, and that auditing capabilities respond as expected in the event of audit record storage capacity could be exceeded.

B.4.5 AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Examine

Review relevant system documentation to obtain an understanding of the organization defined actions to be taken should an audit processing failure occur and the personnel (identified by name or job position) to be notified in the event of an audit processing failure, including audit storage capacity being reached or exceeded.

Review a sample of alerts sent to designated organizational officials due to an audit processing failure. Stopping auditing services on a functional instance of the system may be necessary to obtain these results.

How is an audit failure defined for the system? (e.g., software/hardware errors, failures in the audit capturing mechanisms, audit service errors or faults, failure to write to storage, and audit storage capacity being reached or exceeded, other)?

Test

Arrange to test the audit functions of the system. Work with the ISSO and system administrator to access the audit management console (or other applicable audit features and functions) to ensure that in the event of an audit processing failure, the system alerts designated organizational officials and takes the NRC defined additional actions. If necessary perform these test steps on a non-production instance of the system.

Stop the auditing processes. What happens in the event of audit processing failure? Does the system respond as required?

Does the system alert personnel of an audit processing failure? If so, who is alerted?

Does the system notify the personnel defined by the System Owner or ISSO that are to be alerted in the event of an audit processing failure?

Enhancement 1

Interview

What does the system do in the event of an audit processing failure? Is a warning provided? If so, who is the warning provided to, and at what percentage of the storage capacity threshold?

Examine

Review relevant system documentation to determine whether the system provides a warning when the NRC defined percentage of storage capacity is reached.

Test

Work with the system ISSO and system administrator to exercise audit storage capacity threshold warning functions on the system to ensure warnings are provided when the NRC defined percentage of storage capacity is reached. Observe that warnings are provided (if need be on a test instance of the system) as audit log storage capacity limits are reached. It may be necessary to use a test system and set artificially low capacity limits for testing.

Enhancement 2

Interview

Do any events trigger an immediate alert that the event has occurred? Who is alerted? How soon after the event are they alerted?

Examine

Review relevant system documentation to determine whether the system provides a real time alert in accordance with NRC defined requirements when NRC defined audit failure events occur.

Test

Create or simulate some audit-failure events in a test instance of the system, such as stopping auditing services. Observe the audit management console on the system to ensure the system provides real time alerts in accordance with NRC defined requirements when NRC defined audit failure events occur. Observe alert outputs to ensure they function.

B.4.6 AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Interview

Are system audit records regularly reviewed / analyzed for inappropriate or unusual activity?

How often are the records reviewed and by whom?

Are there records to support that these reviews took place?

Are suspicious activities or suspected violations investigated?

Who is responsible for investigating suspicious activities or suspected violations?

Who does this person report findings to?

What actions are to take place once suspicious activities or suspected violations have been identified?

Examine

Review relevant system documentation to obtain an understanding of the organization’s process for reviewing and analyzing audit records for indications of inappropriate or unusual activity, and for the frequency of the reviews.

Review records to determine whether the organization takes action in response to reports of inappropriate/unusual activities, suspicious behavior, or suspected violations.

Review records that provide evidence that system personnel review and analyze audit records as described in system documentation and in accordance with NRC defined requirements. These records must specify, at a minimum, the name of the individual who reviewed the audit records, the date, and the time of the review.

Review a sample of records that provide evidence that system personnel and/or ISSO investigate and properly report suspicious events, activities, or violations with regard to the system or its data in accordance with NRC defined requirements.

Enhancement 1

Interview

Have automated mechanisms been integrated to the audit monitoring, analysis, and reporting?

What are these mechanisms?

Do mechanisms provide a process for the overall investigation and response to suspicious activities? If so, how?

Examine

Review relevant system documentation and records to determine whether the organization uses automated mechanisms to integrate audit review, analysis, and reporting activities into the organization's overall process for investigation and response to suspicious activities.

Test

Define and run an example audit and reporting scenario looking for a pre-defined series of audit events of interest on the system. Observe automated auditing mechanisms perform to ensure that audit monitoring, analysis, and reporting processes function together as required by collecting the necessary audit data and support organizational processes for investigation and response to suspicious activities.

Enhancement 3

Interview

Does your organization analyze and correlate audit records across different repositories to gain organization wide situational awareness? If so, how is the analysis conducted, and who participates in the analysis? Are the results of the analysis documented?

Examine

Review organization records to determine whether the organization analyzes and correlates audit records across different repositories to gain organization wide situational awareness.

Test

Define and run an example audit and reporting scenario looking for a pre-defined series of audit events of interest on the system. Observe automated auditing mechanisms, such as any automated audit-log correlation capabilities, to ensure the automation allows the organization to analyze and correlate audit records across different repositories to gain organization wide situational awareness. For example the testing could include searching for given user sessions as they move through the organizations networks and finally into the application and database.

Enhancement 5

Interview

During the analysis of audit records, does your organization consider information from other sources? If so, what are the sources?

Examine

Inspect automated auditing mechanisms to determine whether the organization integrates audit information with NRC defined information from other sources.

Test

Work with the ISSO and system administrator staff to locate and observe automated auditing mechanisms to ensure the organization integrates audit information with NRC defined information from other appropriate sources. Locate and verify the input or data collection methods for each other source or log data collector required for the system and verify that each is functional.

Enhancement 6

Interview

During the analysis of audit records, does your organization consider information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity? What information concerning physical access is considered?

Examine

Review organization records to determine whether the organization correlates information obtained from monitoring physical access with information in system audit logs to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

B.4.7 AU-7 AUDIT REDUCTION AND REPORT GENERATION

Interview

Does the system provide an audit reduction and report generation capability?

How does the system perform audit reduction and what is the outcome?

Does the system perform audit reduction without altering the original records?

What kind of audit reports are generated by the system?

Does the system utilize a tool for this function?

If so, what is the tool?

Is the content to be captured in audit records configured from a central location?

Examine

Review relevant system documentation to determine whether the organization uses audit reduction and report generation tools to support on demand audit review and after the fact investigation of security incidents without altering original audit records.

Test

Using a sampling of audit log event files or records, access exercise and observe the automated auditing mechanisms to ensure that the system provides an audit reduction and report capability that is sufficient to support on demand audit review, analysis, and reporting requirements and after the fact investigations of security incidents, and does not alter the original content or time ordering of audit records.

Enhancement 1

Interview

Does the system provide the capability to automatically process audit records for events of interest based on selectable event criteria? If so, what are the events?

Examine

Review specifications for automated mechanisms to determine whether the mechanism provides the ability to automatically process audit records for events of interest as defined in CSO-STD-0020.

Test

Work with the ISSO and system administrator staff as needed to perform test use of the automated auditing mechanisms to ensure the system automatically processes audit records for NRC defined events of interest based on selectable event criteria. The automated tools should successfully locate and process audit records of interest as the tools are operated using event selection criteria known to be valid for that system.

B.4.8 AU-8 TIME STAMPS

Interview

What is the authoritative time source used by the system to generate time stamps?

Examine

Review a sample of audit records on the system to ensure that the system uses internal system clocks to generate time stamps for audit records.

Test

Observe automated auditing mechanisms to ensure the system i internal system clocks generate time stamps for audit records as required. Check the target system and its time source are operating at the same time, and inspect the new audit record entries created to ensure they contain a time-stamp value falling within an acceptable tolerance range without any unacceptable deviation.

Enhancement 1

Examine

Review system-specifications to determine whether the organization synchronizes internal system clocks with the NRC defined authoritative time source in accordance with the NRC defined frequency.

Test

Observe the audit capabilities on the system to verify that the system synchronizes internal system clocks with the NRC defined authoritative time source in accordance with the NRC defined frequency.

B.4.9 AU-9 PROTECTION OF AUDIT INFORMATION

Interview

Is access to audit records protected?

How is audit information (e.g., audit records, audit settings, and audit reports) protected from unauthorized access, modification, and deletion?

How are the tools protected from unauthorized access and modifications?

Examine

Review relevant system documentation to obtain an understanding of the organization's approach to the protection of audit information.

Test

Working with the ISSO and system administrator and written authorization attempt access to the systems audit records. Use accounts that are authorized and should not be authorized to access or read audit records and tools. Verify the system protects the files and tools from any unauthorized read or other access. Verify that audit information and audit tools are protected from unauthorized access, modifications, and deletion.

Enhancement 2

Interview

How are audit records backed up? Where are the backups stored?

Examine

Examine a sample of applicable backup records and/or backup media to determine whether the system backs up audit records onto a physically different system or system component than the system or component being audited in accordance with the NRC defined frequency.

Test

Verify the creation of audit data backups and that the system backs up audit records onto a physically different system or system component than the system or component being audited in accordance with the NRC defined frequency.

Enhancement 3

Interview

Are cryptographic mechanisms used to protect the integrity of audit information and audit tools? If so, what mechanisms are used?

Examine

Review relevant system documentation to determine whether the organization uses cryptographic mechanisms to protect the integrity of audit information and audit tools.

Test

Work with the ISSO and system administrator to access and verify the properties and status of a sampling of production audit log files and verify they are encrypted properly. Verify that adequate cryptographic mechanisms are used to protect the integrity of audit information and audit tools.

Inspect a sampling of production audit log files to determine the qualities of the crypto used (strength, FIPS-140-2 etc.). Verify the audit records produced are protected by cryptographic mechanisms that are FIPS-140-2 validated and using the correct strength, and as per NRC requirements

Enhancement 4

Interview

Who is authorized to manage audit functionality?

Examine

Review relevant system documentation to determine whether only NRC defined privileged users have access to audit functionality on the system.

Test

Work with the ISSO and system administrator to test and observe the use of system accounts that should have access to automated auditing mechanisms to verify that only the assigned NRC defined privileged users may access the audit functionality on the system. Attempt to access the audit mechanisms with a few other unauthorized “admin” accounts to verify unauthorized access attempts are rejected.

B.4.10 AU-10 NON REPUDIATION

Interview

Does the system employ any mechanisms supporting non repudiation? Please describe the mechanism.

Examine

Review relevant system documentation to determine whether the mechanisms are configured to protect against an individual (or process acting on behalf of an individual) falsely denying having performed NRC defined actions.

Test

Examine a sampling of files or messages that should contain digital signatures, to ensure that the system protects against an individual (or process acting on behalf of an individual) falsely denying having performed NRC defined actions.

B.4.11 AU-11 AUDIT RECORD RETENTION

Interview

How long are audit records that contain security incident related information retained for?

How long are all other audit records retained for?

Examine

Select a sampling of points within the expected audit record retention time-period and request or search for the systems audit records from that time to ensure the records are still available and meet the NRC defined time period and records retention policy.

B.4.12 AU-12 AUDIT GENERATION

Interview

How often are audit records generated?

Can specific events be selected for auditing?

Who selects the auditable events?

Examine

Review system audit records to determine:

- Whether the system audits all NRC defined events.
- Whether the events are audited on all NRC defined system components.
- Whether the audit records provide the NRC defined content (AU-3) for each of the NRC defined events (AU-2).

Test

Work with the ISSO and system administrator to use the audit mechanisms and verify that the system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system, throughout the system.

Enhancement 1

Examine

Review the system generated, system wide audit trail to determine whether the system compiles audit records from all NRC defined system components.

Test

Observe the system in use and verify that the system's automated auditing mechanisms compile audit records from NRC defined system components into the system wide audit trail. Verify these records are time correlated to within the NRC defined level of tolerance.

Enhancement 3

Interview

Does the system allow the capability for authorized personnel to change the auditing to be performed?

Who is capable of changing the auditing to be performed?

What circumstances would compel a need to change the auditing to be performed?

Examine

Review relevant system documentation to determine whether the system allows for authorized personnel to change the auditing to be performed in accordance with NRC defined requirements.

Test

On a non-production instance of the system (that matches prod) ask the ISSO and system administrator to login to the systems audit mechanisms using accounts authorized to make changes. Attempt audit function changes, ensuring any change steps are observed and noted. Then check for audit log entries that reflect the changes. Undo any changes.

Using accounts that should not be authorized to make changes to the systems audit mechanisms, work with the ISSO to attempt access and make changes to the audit configurations of audit capabilities on the system to verify that the system only allows for authorized personnel to change the auditing to be performed in accordance with NRC defined requirements.

B.5 SECURITY ASSESSMENT AND AUTHORIZATION (CA)

Security assessment and authorization assessment objects include, but are not limited to: policy and procedures; security assessment plans and reports; interconnection security agreements; system Plans of Action and Milestones (POA&Ms); and tasks performed by organization staff in support of security assessment and authorization functions.

B.5.1 CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Interview

Are system-specific security assessment and authorization policies and procedures available?

Who is responsible for reviewing, updating, and disseminating these procedures?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated security assessment and authorization controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to.

Examine organization records to determine whether or not policy and procedures were disseminated to the organization elements.

Review the system-specific security assessment and authorization policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.5.2 CA-2 SECURITY ASSESSMENTS

Interview

When was the last annual assessment of the security controls in the system conducted? Where is it documented?

Who were the assessment results distributed to? Are there records to demonstrate that they were distributed?

Examine

If the system is undergoing an initial authorization effort, review the security assessment plan developed in support of the SCA-to determine whether the plan is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

If the system is undergoing a reauthorization:

- Review each security assessment plan developed in support of system assessments conducted after receiving the initial authorization to determine whether the plans are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”
- Review each security assessment report to determine the reports are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”
- Review organization records to determine whether the results of the security control assessment were provided to NRC defined individuals (or roles).

Enhancement 1

Interview

Who conducted the assessment?

Examine

Review the security assessment plan and the security assessment report to determine whether the system was assessed by independent assessors in compliance with the NRC defined level of independence.

Enhancement 2

Interview

Does your organization conduct:

- Annual assessments?
- Announced and unannounced assessments?
- In depth monitoring, malicious user testing, penetration testing, or red team exercises?

If so, are records and reports available to demonstrate that these took place?

Examine

Review the security assessment plan and the security assessment report to determine whether the system was assessed at the NRC defined frequency using the NRC defined forms of assessment as defined in CSO-STD-0020.

B.5.3 CA-3 SYSTEM CONNECTIONS

Interview

What systems does your system connect to?

Does your system connect to any external systems, and, if so, does your organization have a signed Interconnection Security Agreement (ISA)?

Who is responsible for reviewing the ISAs? How often are they reviewed?

Does your system connect to any public networks?

Examine

Review relevant system documentation to determine whether the system connects to systems outside of the system's authorization boundary.

Review all organization Interconnection Security Agreements (ISAs) to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, "System Artifact Examination Procedure."

Review organization records to determine whether ISAs have been reviewed, and if applicable, updated per the NRC defined frequency provided in CSO-STD-0020.

Test

Observe relevant system features and functions, such as firewalls or other boundary devices, to ensure that the organization monitors connections to external systems on an ongoing basis to verify enforcement of security requirements.

Enhancement 5

Interview

What type of policy is implemented on the system for restricting external connections (i.e., blacklisting or whitelisting)?

Examine

Review relevant system documentation to determine whether the system restricts external connections in accordance with NRC defined requirements.

Test

Working with the system ISSO and system administrator staff carry out some test connection attempts against the system with an authorized test strategy and tools. Observe the relevant system features and functions, such as firewalls or other boundary devices, to ensure that the system restricts external connections in accordance with NRC defined requirements.

B.5.4 CA-5 PLAN OF ACTION AND MILESTONES

Interview

Has a Plan of Action and Milestones (POA&M) been developed for the system?

How often does your organization update the POA&M?

What circumstances or events prompt you to update the POA&M?

Where does your organization archive/store evidence of POA&M item closures?

Examine

Review the system POA&M to determine:

- Whether the organization tracks all identified weaknesses and required continuous monitoring activities within the POA&M.
- Whether the organization updates the POA&M at the NRC defined frequency defined in CSO-STD-0020 and per the NRC POA&M process, CSO-PROS-2016, “Plan of Action and Milestones Process.”

B.5.5 CA-6 SECURITY AUTHORIZATION

Interview

Has your system been authorized by the DAA? If so, please provide the authorization approval memo and supporting authorization assessment reports.

Examine

If the system is undergoing an initial authorization effort, no authorization assessment objects are available to review.

If the system is undergoing a reauthorization effort, review every authorization approval memo issued to the organization by the DAA to determine:

- Whether the DAA authorized operation before the system commenced operations.
- Whether the organization was reauthorized for operation at the NRC defined frequency as communicated by the DAA in each authorization approval memo.

B.5.6 CA-7 CONTINUOUS MONITORING

Interview

What continuous monitoring activities take place to support an ongoing awareness of threats, vulnerabilities, and information security (and support organizational risk management decisions)? Please describe each activity.

How is the security related information obtained during continuous monitoring activities communicated to NRC officials? Who is it communicated to?

Examine

Review all system documentation developed in support of continuous monitoring activities (e.g., the SSP, security assessment plans and reports, periodic vulnerability scan reports) to determine:

- Whether all NRC defined continuous monitoring activities have been completed at the NRC defined frequency.
- Whether the organization monitors NRC defined metrics in accordance with the NRC continuous monitoring strategy.
- Whether all NRC defined assessment activities have been completed at the NRC defined frequency.

Examine organization records to determine whether:

- The organization correlates and analyzes security related information generated by assessments and monitoring.
- The organization takes action to respond to the results of the analysis.
- The organization reports the security state of the organization and system to NRC defined personnel at the NRC defined frequency.

Enhancement 1

Interview

Are security control assessments conducted by independent assessors?

Examine

Examine organization records, correspondence, and assessment plans to determine whether the continuous monitoring of security controls is conducted on an ongoing basis by independent assessors.

B.5.7 CA-8 PENETRATION TESTING

Interview

Has penetration testing been performed on the system?

When was penetration testing last performed?

Where are the results of penetration testing documented?

Examine

Review organization records and system documentation that demonstrates that penetration testing has been performed on NRC defined system components at the NRC defined frequency.

B.5.8 CA-9 INTERNAL SYSTEM CONNECTIONS

Interview

Who authorizes internal connection of devices to your system? Which devices must be authorized?

Are the connections documented? If so, please provide the documentation for review.

Examine

Review relevant system documentation and organization records to determine:

- Whether the organization explicitly authorizes internal connections of NRC defined system components to the system.
- Whether the organization documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

B.6 CONFIGURATION MANAGEMENT (CM)

Configuration management assessment objects include, but are not limited to: policy and procedures; configuration management plans; the baseline configuration of the system; system architecture and configuration documentation; historical copies of baseline configurations; and tasks performed by organization staff in support of configuration management functions.

B.6.1 CM-1 CONFIGURATION MANAGEMENT POLICIES AND PROCEDURES

Interview

Are system-specific configuration management policies procedures available?

Who is responsible for reviewing, updating, and disseminating these procedures?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Examine organization records to determine whether the policy was reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated configuration management controls.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to.

Examine organization records to determine whether or not policy and procedures were disseminated to the organization elements.

Review the system-specific configuration management policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.6.2 CM-2 BASELINE CONFIGURATION

Interview

Has a baseline configuration been established for the system?

Has this baseline been documented?

Who is responsible for maintaining the system baseline configuration?

Does your organization have approved deviations or waivers for all deviations from NRC required configuration settings?

Examine

Review relevant system documentation to determine:

- Whether the organization develops and documents and maintains a current baseline configuration of the system.
- Whether deviations to the baseline configuration are documented.
- Whether the baseline configuration is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

Enhancement 1

Interview

Is the baseline updated as needed to reflect the current configuration of the system?

Examine

Review the current and historical baseline configurations to determine whether the organization updates the baseline configuration:

- at the NRC defined frequency.
- Due to NRC defined circumstances.
- Whenever system components are installed or upgraded.

Enhancement 2

Interview

Does the system use an automated mechanism to maintain the configuration baseline?

Examine

Review relevant system documentation to determine whether the organization uses automated mechanisms to maintain an up to date, complete, accurate, and readily available baseline configuration of the system.

Test

Working with the system's ISSO and/or system administrator observe the configuration baseline automated mechanisms in use such as during the creation of a new or updated system baseline. Verify these mechanisms are effective to keep the baseline configuration kept up to date, complete, accurate, and readily available.

Inspect a sampling of stored baseline files and records and compare with the current baseline properties and change log entries to ensure the baseline image, files, or data set is current reflecting the current configuration.

Enhancement 3

Interview

How long does your organization retain the baseline to support system rollbacks?

What is included in the baseline?

Examine

Review a sample of previous versions of the baseline configuration to ensure that the organization retains previous versions of baseline configurations in accordance with NRC defined requirements to support rollback.

Enhancement 7

Interview

Does your organization issue laptops to system staff traveling to locations that the organization deems to be of significant risk?

If so, what is your process for applying safeguards to the laptops when they are returned? Is the process documented?

Examine

Review relevant system documentation to ensure that components or devices used to travel to locations that the organization deems to be of significant risk are configured in accordance with NRC defined requirements.

Test

Inspect a sample of NRC defined components or devices used to travel to locations that the organization deems to be of significant risk and compare their present configuration baseline with the CSO required configuration baseline to ensure they are being configured in accordance with NRC defined requirements.

B.6.3 CM-3 CONFIGURATION CHANGE CONTROL

Interview

Does your organization have a process for managing configuration changes?

If so, what is the name of the process?

Does your organization audit activities associated with configuration changes to the system?

How are changes to each configuration item authorized?

How are the changes to configuration items documented?

Who is responsible for controlling changes to the system?

Are there records to support that changes were reviewed and authorized?

Do the approvals to implement a change to the system include successful results from a security analysis of the change?

Examine

Review the organization’s configuration management policy and procedures to obtain an understanding of the organization’s process for managing configuration changes.

Review relevant system documentation to determine the types of changes to the system that are configuration controlled.

Review recently proposed configuration controlled changes to the system to determine whether the organization explicitly approves or disapproves changes based on a formal security impact analysis.

Review organization records and system documentation to determine:

- Whether configuration change decisions are formally documented.
- Whether approved changes were made to the system.
- Whether records of the configuration controlled changes were retained for the NRC defined time period.
- Whether the organization audits and reviews activities associated with configuration controlled changes to the system.

- Whether the organization coordinates and provides oversight for configuration change control activities through NRC defined change control elements that convene at the NRC defined frequency or under NRC defined conditions.

Test

Inspect audit records captured and stored by the system’s audit capabilities to ensure that the system audits activities associated with configuration controlled changes to the system. Compare a sampling of live audit record entries to the requirements of current CSO standards and document the results.

Enhancement 1

Interview

Does the system employ automated mechanisms to track proposed configuration changes? If so, what mechanism is used?

Does the tool notify appropriate approval authorities? If so, how?

Does the tool highlight approvals that have not been received in a timely manner?

If so, what is the timeframe for approvals and where is it documented?

Does the tool prohibit changes to the system until necessary approvals are received?

Does the tool document completed changes to the system?

Does the tool notify approval authorities when the changes are implemented?

Examine

Review relevant system documentation to determine whether the organization employs automated mechanisms to:

- Document proposed changes to the system;
- Notify NRC defined authorities of proposed changes to the system and request change approval;
- Highlight proposed changes to the system that have not been approved or disapproved by the NRC defined time period;
- Prohibit changes to the system until designated approvals are received;
- Document all changes to the system; and
- Notify NRC defined personnel when approved changes to the system are completed.

Test

Working with the system staff attempt to submit a new sample change request through the automated system change process. Observe automated configuration change tracking mechanisms to determine if the organization’s automated mechanisms document proposed changes to the system in accordance with NRC defined requirements.

Arrange to view the change management automation console of any applicable automated configuration change tracking mechanisms. Look for visual evidence and/or past records to verify the mechanisms do highlight proposed changes that have not been approved or disapproved within the NRC defined timeframe, or for any change requests that are late or past-due.

Observe the automated configuration change tracking mechanisms while in use to ensure that the system notifies NRC defined personnel when approved changes to the system are completed. It may be necessary for the assessors to ask the team to process sample change requests to test these functions.

Enhancement 2

Interview

Does your organization test, validate, and document changes to the system before implementing the changes on the operational system? Where are the changes tested? Are test results documented? If so, where?

Examine

Review a sample of change requests or other relevant documentation to ensure that the organization tests, validates, and documents changes to the system before implementing the changes on the operational system.

B.6.4 CM-4 SECURITY IMPACT ANALYSIS

Interview

Does your organization analyze changes to the system to determine the security impact of the changes before implementing them?

Who conducts the security impact analysis? Where is the analysis documented?

Have specific types of changes been identified that must be analyzed? If so, what are those changes and are they documented?

Are the security features that could be impacted by the change documented? If so where?

Examine

Examine system documentation such as change control records, historical configuration baselines, and system audit records to determine whether changes were made to the system.

Review each documented security impact analysis supporting the identified changes to determine whether they are documented, reviewed, and approved in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

Enhancement 1

Interview

Are the changes (including upgrades and modifications) tested, and are security features checked to verify that the features are still functioning properly? If so, where are the changes tested?

Is there a documented process/procedure for verifying the proper functioning of the security features?

Who tests the security features, and where are the test results documented?

Examine

Review organization records to determine whether the organization analyzes changes in a separate test environment before implementation in the operational environment.

Review organization records to determine whether there is a documented process/procedure for verifying proper functioning of the security features.

Review organization records to determine whether test results were formally documented.

B.6.5 CM-5 ACCESS RESTRICTIONS FOR CHANGE

Interview

Who is authorized to access the system for the purpose of making changes?

Who approves access privileges for the individuals? Is a documented list of authorized individuals maintained?

How are physical and logical access restrictions associated with changes to the system enforced?

Are records regarding the changes to the system generated, retained, and reviewed?

Who is responsible for generating, retaining, and reviewing records reflecting all such changes to the system?

Are there records to support that these reviews and updates took place?

Examine

Review system configuration management documentation to determine whether the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the system.

Test

Working with the system ISSO and system administrator staff login to the system (or a test instance) with a sampling of account types, (non-privileged), and attempt to make changes. Observe a sample of logical access enforcement mechanisms or other applicable software features or functions to ensure that only NRC defined and authorized privileged users can use their logical access to make changes to the system.

Inspect the physical access enforcement mechanisms of the system environment to ensure that only NRC defined privileged users have physical access to make changes to the system. Ensure any physical access approval roster or badge entries present in the system reflect current and appropriate access approvals.

Enhancement 1

Interview

Does the system enforce access restrictions and support auditing of the enforcement actions?

Examine

Review system audit logs to determine whether access restrictions are enforced and logged.

Test

Working with the appropriate site officials to organize approved testing, attempt access to the facility or room with a sampling of inappropriate or expired credentials, and/or outside of approved access hours and days, etc. Observe automated access enforcement mechanisms to ensure that the system enforces access restrictions, rejecting any inappropriate after-hours access attempts (as defined by policies), expired or disabled badges, badges of terminated employees or contractors, etc.

Following the access attempts above inspect of the systems access audit records to ensure the system supports auditing of the access enforcement actions per applicable requirements.

Enhancement 2

Interview

How often does your organization review changes to determine whether unauthorized changes have occurred? What circumstances would prompt you to review changes?

Examine

Review organization records to determine whether the organization reviews system changes at the NRC defined frequency and under NRC defined circumstances to determine whether unauthorized changes have occurred.

Enhancement 3

Interview

Does the system verify that a component has been digitally signed using a certificate that is recognized and approved by your organization before installing the component?

Examine

Review relevant system documentation to determine whether the system prevents the installation of NRC defined critical software programs that are not signed with a certificate that is recognized and approved by the organization.

Test

Working with the system ISSO and system administrator team attempt to install a sample of NRC defined critical software programs that are not signed with a certificate that is recognized and approved by the organization. Verify the system functions to ensure installation of these programs is prevented.

Inspect the system to verify that any programs, software, or firmware already installed meets current NRC code-signing certificate policies.

B.6.6 CM-6 CONFIGURATION SETTINGS

Interview

Have the security configuration settings been set to the most restrictive mode that is consistent with operational requirements?

Where are the security configuration settings documented?

How does your organization enforce the configuration settings in all components of the system?

Examine

Review the results of vulnerability scans and system configuration checks to determine whether security configuration settings have been set to the most restrictive mode consistent with operational requirements and NRC configuration standards.

Review all approved deviations and waivers to determine whether the organization identifies and documents deviations from established configurations for all NRC defined system components based on NRC defined operational requirements, and submits them to the DAA for approval.

Review relevant system documentation to determine whether the organization monitors and controls changes to configuration settings in accordance with NRC policies and procedures.

Test

Using NRC and system ISSO/system administrator approved test approach and tools, as appropriate, performing hardening checks for all applicable system components. Determine if the system components are hardened per NRC policy.

Enhancement 1

Interview

Does the system employ automated mechanisms to centrally manage, apply, and verify configuration settings?

Examine

Review system configuration management documentation to determine whether the organization uses automated mechanisms to centrally manage, apply, and verify configuration settings.

Test

Working with the appropriate system team members login to the automated change management mechanisms and demonstrate the operation of it. Inspect, and observe use of the automated change management mechanisms to verify the system's configuration settings are centrally managed, applied, and verified for NRC defined system components. Where necessary an assessor may request a walk-through of entering and processing a sample change.

Enhancement 2

Interview

What safeguards are employed to respond to unauthorized changes to configuration settings?

Examine

Review organization records of unauthorized changes to determine whether the organization employs NRC required safeguards when responding to unauthorized changes to NRC defined configuration settings.

Test

Observe automated change management mechanisms or other applicable system features or functionality to ensure that the system employs NRC defined safeguards to respond to unauthorized changes to configuration settings for NRC defined system components.

B.6.7 CM-7 LEAST FUNCTIONALITY

Interview

What functions, ports, protocols, and services have been defined as prohibited and/or restricted for the system? Where is this documented?

Is the system configured to provide only essential capabilities? If so, how? Where is this documented?

How does the system prohibit and/or restrict the use of prohibited and/or restricted functions, ports, protocols, and/or services? Where is this documented?

Does the organization limit component functionality to a single function per device when feasible? Where is this documented?

Examine

Review the results of vulnerability scans and system configuration checks to determine whether the system non-essential capabilities are available, or restricted or prohibited functions, ports, protocols, and/or services are enabled.

Test

Using NRC approved tools and working with the ISSO and system administrator access and assess the systems current configuration. Compare the configurations of applicable system components with approved requirements to verify that only essential NRC approved capabilities are provided to users of the system.

Using NRC approved tools and working with the ISSO and system administrator access and assess the systems current configuration. Compare the configurations of applicable system components to verify that only approved functions, ports, protocols, and services are allowed on the system, and that the system-specifically prohibits or restricts the use of NRC defined functions, ports, protocols, and services prohibited for use on the system by NRC policies

Enhancement 1

Interview

Are system functions and services reviewed for possible elimination? How often are they reviewed? Are there records to support that the reviews took place?

Who is responsible for reviewing and determining which functions and services are candidates for elimination?

Is there a process or checklist for the review of system functions and services reviewed for possible elimination?

Examine

Review organization records to determine:

- Whether the organization inspects system components for unnecessary or non-secure functions, ports, protocols, and services at the NRC defined frequency.
- Whether the organization disables NRC defined unnecessary or non-secure functions, ports, protocols, and services.

Enhancement 2

Interview

Does the system prevent program execution in accordance with NRC rules authorizing the terms and conditions of software program usage?

Examine

Review relevant system documentation to determine whether the system prevents program execution in accordance with NRC defined requirements.

Test

Working with the ISSO and system administrator identify example programs or software that users or unauthorized accounts or processes should not be able to execute on the system, per NRC policies. Attempt to run the programs and observe whether the automated mechanisms prevent execution of the unauthorized software in accordance with NRC defined requirements. Use the systems program or task manager tools and/or system logs and consoles as needed to identify running programs to confirm.

Enhancement 4

Interview

Does your organization identify all software programs that are not authorized to execute on the system? If so,

Does your organization employ an allow all, deny by exception policy to prohibit the execution of unauthorized software programs on the system; and

Does your organization review and update the list of unauthorized software programs? How often are they reviewed? Who is responsible for reviewing them? Are there records to support that the reviews took place?

Examine

Review relevant system documentation to determine:

- Whether the organization identifies all software programs that are not authorized to execute on the system.
- Whether the organization employs an allow all, deny by exception policy to prohibit the execution of unauthorized software programs on the system.

Review organization records to determine whether the organization reviews and updates the list of unauthorized software programs at the NRC defined frequency.

Test

Work with the ISSO and system administrator to identify example blacklisted or unauthorized software that is safe for these control testing purposes (only) on a non-production but similar instance of the system. Note: Any blacklisted software used for this testing must meet all other NRC software security requirements, be scanned and verified as non-infected, not containing malware or malicious code, and cannot be able to “hide” on the system.

Attempt to execute the example (blacklisted) programs on the non-production system and observe whether the automated mechanisms prevent execution of the blacklisted software in accordance with NRC defined requirements and policies. If the software installs, changes, and/or executes on the system in any way this control test fails.

Verify the system’s automated program execution controls enforce current NRC allow all, deny by exception (blacklisting) policies (as applicable) to prohibit the execution of unauthorized software programs on the system. If the software installs, changes, and/or executes on the system this test fails.

Use the system’s program manager, or task manager tools, console utilities, and/or system logs as needed to verify the unauthorized programs are not running.

Enhancement 5

Interview

Does your organization identify all software programs that are authorized to execute on the system?

Does your organization employ a deny all, permit by exception policy to allow only the execution of authorized software programs on the system; and

Does your organization review and update the list of authorized software programs? How often are they reviewed? Who is responsible for reviewing them? Are there records to support that the reviews took place?

Examine

Review relevant system documentation to determine:

- Whether the organization identifies all software programs that are authorized to execute on the system.
- Whether the organization employs a deny all, permit by exception policy to allow only the execution of authorized software programs on the system.

Review organization records to determine whether the organization reviews and updates the list of authorized software programs at the NRC defined frequency.

Test

Work with the Work with the ISSO and system administrator to identify any non-whitelisted (in this case unauthorized) software that is safe for these control testing purposes (only) on a non-production but similar instance of the system. Note: Any non-whitelisted software used for this testing must otherwise meet all NRC software security requirements, be scanned and verified as non-infected, not containing malware or malicious code, and cannot be able to “hide” on the system.

Attempt to execute the example unauthorized programs on the non-production system instance and observe whether the automated mechanisms prevent execution of the unauthorized software in accordance with NRC defined requirements and policies. If the software installs, changes, and/or executes on the system in any way this control test fails.

Verify the system’s automated program execution controls enforce current NRC deny all, allow by exception (whitelisting) policies (as applicable) to prohibit the execution of unauthorized software programs on the system. If the software installs, changes, and/or executes on the system this test fails.

Use the system’s program manager, or task manager tools, console utilities, and/or system logs as needed to verify the unauthorized programs are not running.

B.6.8 CM-8 SYSTEM COMPONENT INVENTORY

Interview

Does your organization have a current inventory of all system components? Where is the inventory documented?

How often does your organization review and update the inventory?

Who is responsible for reviewing and updating the inventory to keep it up to date?

Who is responsible for maintaining the inventory?

Are all components within the system’s authorization boundary included in the inventory?

Examine

Review the system component inventory to determine:

- Whether the inventory is complete and current (as compared to the documented configuration baseline, system architecture, approved change requests, etc.).
- Whether all components within the system's authorization boundary are listed in the inventory.
- Whether the inventory provides all NRC defined information deemed necessary to achieve effective accountability.
- Whether virtual servers and components are reflected in the inventory.

Review organization records to determine whether the organization reviews and updates the system component inventory at the NRC defined frequency.

Review the system hardware and software component inventory to determine whether the inventory is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, "System Artifact Examination Procedure."

Enhancement 1

Interview

What circumstances or events prompt you to update the system inventory?

Examine

Review NRC records of component installations, removals, and updates to determine whether they are reflected in the inventory.

Enhancement 2

Interview

Does the system employ automated mechanisms to help maintain the system inventory?

Examine

Review relevant system documentation to determine whether the system uses automated mechanisms to help maintain the system inventory.

Test

Work with the ISSO, system administrator and/or system team and perform adequate research to understand the capabilities, configuration, and functions of any automated inventory mechanisms used to help maintain inventory of the system.

Based on the inventory mechanisms expected capabilities access and observe the operation of or inspect the automated inventory mechanisms used to maintain the system component inventory to verify that the system inventory is kept up to date, complete, accurate, and readily available. Compare the records collected and maintained by the mechanisms with the current as-built production system inventory to verify accuracy. Verify the tools and records account for all system inventory items, noting if any manual steps are required to add any objects that cannot be automatically inventoried.

Select an example set of recent system inventory changes if available. Inspect these records to verify accuracy and to ensure the automated mechanisms processed the inventory changes correctly.

If pre-existing records are lacking and/or if necessary work with the ISSO and system administrator to attempt a test inventory change (to a non-production system as needed) and verify the automated inventory mechanisms respond to and track the change as intended.

Enhancement 3

Interview

Does the system employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the system? If so, how often does the mechanism check for unauthorized components?

What does the system do when unauthorized components are detected?

Examine

Review relevant system documentation to determine whether the system uses any automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components.

Test

Work with the system ISSO and system administrator to understand and test the automated unauthorized component mechanisms, such as network access control technology. Attempt to add or connect unauthorized components to the system and verify that the system automatically detects the presence of the unauthorized hardware, software, or firmware components within the system (as designed) and takes the NRC defined action when unauthorized components are discovered.

Enhancement 4

Interview

Does the inventory indicate who is responsible for maintaining each component?

Examine

Review the inventory to determine whether the individuals responsible for administering each component are identified.

Enhancement 5

Interview

Does your organization verify that the components within the authorization boundary of your system are not also reported in other system inventories? If so, what is your process for doing so?

Examine

If possible, review the inventory of a sample of interconnected systems to determine whether components within the system's authorization boundary are reported in other system inventories.

B.6.9 CM-9 CONFIGURATION MANAGEMENT PLAN

Interview

Does your organization have a configuration management plan for the system?

Who is responsible for maintaining the plan?

Who is responsible for placing configuration items under configuration management?

Examine

Review the system Configuration Management Plan to determine:

- o Whether the plan addresses roles, responsibilities, and configuration management processes and procedures.
- o Whether the plan establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the items.
- o Whether the plan defines the configuration items for the system, and places the items under configuration management.
- o Whether the plan provides instructions for protecting the plan from unauthorized disclosure and modification.

Review the system Configuration Management Plan to determine whether the plan is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, "System Artifact Examination Procedure."

Test

Work with the ISSO, system administrator, and CM-team as needed to attempt access to the plan with accounts that might have access to read or download the CM-plan document but should not be able to. Verify that the access enforcement mechanisms used to limit access to the plan itself protect the CM-plan from any unauthorized disclosure and modification.

B.6.10 CM-10 SOFTWARE USAGE RESTRICTIONS

Interview

Does your organization track the use of software and associated documentation protected by quantity licenses to control copying and distribution? If so, who is responsible for doing so?

What is the process for tracking this?

Is the process documented?

Does your organization control and document the use of peer to peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work?

If so, who is responsible for doing so?

What is the process for controlling this?

Is the process documented?

Examine

Review relevant system documentation to:

- Obtain an understanding of the organization’s approach to software usage restrictions,
- Determine whether the organization uses software and associated documentation in accordance with contract agreements and copyright laws, and to obtain an understanding of the organization’s approach to software usage restrictions, and
- Determine whether the organization has a documented process for controlling use of peer to peer file sharing technology.

Examine organization records to determine whether the organization:

- Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
- Documents the use of peer to peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Test

Scan the configurations of system components or audit with NRC approved tools and CSO procedures to verify that peer to peer file sharing technology is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

B.6.11 CM-11 USER INSTALLED SOFTWARE

Interview

Does your organization have policies governing the installation of software by users?

If so, how does your organization enforce the software installation policies?

How often does your organization monitor for compliance with the policy?

Examine

Review relevant system documentation to:

- Determine whether the organization has established a policy governing the installation of software by users.
- Obtain an understanding of the organizations approach to enforcing the policy.

Examine organization records to determine whether the organization monitors for compliance with the policy at the NRC defined frequency.

Test

Work with the ISSO and system administrator to verify that the system enforces software installation policies in accordance with NRC defined requirements, as follows:

Work with the ISSO and system administrator to identify examples of unauthorized software that is safe for only for control testing purposes on an adequately similar non-production instance of the system. Note: Any software used for this testing must otherwise meet all NRC software security requirements, be scanned and verified as non-infected, not containing malware or malicious code, and cannot be able to "hide" on the system.

Attempt to install the example unauthorized programs on the non-production system instance and observe whether the automated software restriction mechanisms monitor and prevents installation of any unauthorized software by users and in accordance with NRC defined requirements and policies. If the software installs on or changes the system in any way this control test fails.

Use the system's program manager, console utilities, policy manager logs and/or system logs as needed to verify the unauthorized programs are not installed.

B.7 CONTINGENCY PLANNING (CP)

Contingency planning assessment objects include, but are not limited to: policy and procedures; contingency plans, contingency test plans and contingency test reports; and tasks performed by organization staff in support of contingency functions.

B.7.1 CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Interview

Are system-specific contingency policies and procedures available?

Who is responsible for reviewing, updating, and disseminating these procedures?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated contingency planning controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific contingency planning policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.7.2 CP-2 CONTINGENCY PLAN

Interview

Has a contingency plan for the system been developed?

Has the contingency plan been reviewed and approved by designated organizational officials?

Who is responsible for reviewing and approving the contingency plan?

Were contingency planning activities coordinated with incident handling activities? If so, how?

Are there records to support that the review and approvals have occurred?

Are there records to support that the contingency plan been disseminated to key contingency personnel?

Have key contingency personnel and the key operating elements acknowledged they understand the contingency plan and are ready to implement the plan?

Are there records to support that personnel and key operating elements have acknowledged they understand the contingency plan and are ready to implement the plan?

How often does your organization review and update the contingency plan? What circumstances or events prompt an update?

Who does your organization communicate contingency plan changes to?

Examine

Review the system contingency plan to determine whether the plan:

- Identifies essential missions and business functions and associated contingency requirements;
- Provides recovery objectives, restoration priorities, and metrics;
- Addresses contingency roles, responsibilities, assigned individuals with contact information;
- Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
- Addresses eventual, full system restoration without deterioration of the security safeguards originally planned and implemented.
- Provides instructions for protecting the plan from unauthorized disclosure and modification.

Review the system contingency plan to determine whether the plan is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, "System Artifact Examination Procedure."

Examine organization records to determine whether:

- The plan was reviewed and approved by NRC defined personnel (or roles).
- The plan was distributed to NRC defined key contingency personnel and organizational elements.
- Planning activities were coordinated with incident handling activities.
- The organization reviewed the contingency plan at the NRC defined frequency.
- The organization updated the contingency plan to address changes to the organization, system, or environment of operation.
- The organization updated the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.
- The organization communicated changes to the plan to NRC defined key contingency personnel and organizational elements.

Enhancement 1

Interview

Does your organization coordinate the development of the contingency plan with other organizations responsible for related plans? If so, which organizations, and which plans?

Examine

Examine organization records to determine whether the organization coordinates the development of the contingency plan with other organizations responsible for related plans.

If possible, review the contingency plans for the other organizations to determine whether they indicate that coordination took place.

Enhancement 2

Interview

Does your organization conduct capacity planning? If so, what does that entail?

Examine

Examine organization records to determine:

- Whether capacity planning was conducted.
- Whether capacity for information processing, telecommunications, and environmental support during contingency operations was addressed during planning.

Enhancement 3

Interview

What is the planned timeframe for resuming essential missions and business functions after the contingency plan is activated?

Examine

Review the contingency plan to determine whether the planned timeframe for resuming essential missions and business functions after the contingency plan is activated aligns with the NRC defined time period.

Enhancement 4

Interview

What is the planned timeframe for resuming all missions and business functions after the contingency plan is activated?

Examine

Review the contingency plan to determine whether the organization plans for the resumption of all missions and business functions within the NRC defined time period of contingency plan activation.

Enhancement 5

Interview

How does your organization plan for the transfer of essential missions and business functions to alternate processing and/or storage sites?

Examine

Review the contingency plan to determine whether the organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Enhancement 8

Interview

What missions and business functions does your organization consider to be critical? Which system assets support the missions and functions? Has your organization employed additional safeguards and countermeasures to protect the assets?

Examine

Review the contingency plan, and, if available, the system business impact analyses to determine whether the organization identifies critical system assets supporting essential missions and business functions.

Work with the ISSO and system administrator as needed to Examine the system configuration and operations to determine if any additional safeguards and countermeasures documented in the plan could be considered implemented or not.

B.7.3 CP-3 CONTINGENCY TRAINING

Interview

Does your organization conduct contingency training? How often?

Who participates in the training? How long after an individual assumes a contingency role or responsibility is training conducted?

What changes to the system would prompt contingency training?

Does your organization keep records of the training? If so, please provide the records.

Examine

Examine organization records to determine whether:

- The organization provides contingency training to system users consistent with assigned roles and responsibilities.
- Training is provided within the NRC defined timeframe of assuming a contingency role or responsibility.
- Training is provided when required by system changes.
- After initial training, verify the organization provides training at the NRC defined frequency.

Enhancement 1

Interview

Does your organization incorporate simulated events into contingency training? If so, what type of events have been simulated?

Examine

Review training materials to determine whether the organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

B.7.4 CP-4 CONTINGENCY PLAN TESTING

Interview

How often does your organization test the contingency plan?

Who is responsible for reviewing the test results, and for initiating corrective actions?

Are the corrective actions documented? If so, where?

Examine

Review all historical contingency test plans and contingency test reports to determine whether the organization tests the contingency plan for the system:

- at the NRC defined frequency, and

- Using NRC defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan.

Review all historical contingency test plans and contingency test reports to determine whether the organization tests the contingency plan and documents the results in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

Examine organization records to determine whether:

- Contingency Plan Test Results were reviewed.
- Corrective actions were taken, if applicable.

Review the contingency plan to determine whether updates to the plan were made as a result of testing (if applicable).

Enhancement 1

Interview

Does your organization coordinate testing with other organizations? Which organizations? Are there records to support that coordination took place?

Examine

Examine organization records to determine whether the organization coordinated testing of the contingency plan with other organizations responsible for related plans.

If possible, review contingency test reports for the other organizations to determine whether the reports indicate that coordination took place.

Enhancement 2

Interview

Does your organization test the contingency plan at the system’s alternate processing site? If so, how often? Are there records to support that the testing took place?

Examine

Review contingency test plans and contingency test reports to determine whether the organization tested the contingency plan at the alternate processing site, and in accordance with current NRC contingency plan testing policies and criteria.

B.7.5 CP-6 ALTERNATE STORAGE SITE

Interview

Has your organization established an alternate storage site? If so, have agreements been established to permit the storage and retrieval of system backup information?

What information security safeguards are provided at the alternate site? Are they documented in the agreement?

Examine

If the organization has established an alternate storage site, review the agreement established with the site to:

- Determine whether the agreement supports the storage and retrieval of system backup information.
- Determine whether the information security safeguards are documented in the agreement.
- Determine whether the safeguards planned are equivalent to that of the primary site.

Enhancement 1

Interview

Where is the alternate site located?

Do all personnel identified in the contingency plans know where and how to access backup and recovery media stored at the alternate site if required to do so?

Examine

Review the contingency plan and the agreement with the alternate storage site to determine whether the site is located at a distance sufficient from the primary site to reduce susceptibility to the same threats.

Examine records of what personnel from the organization are currently authorized to access the backup and recovery media at the alternate site against the current list of personnel assigned to the system. Verify that only the correct current personnel are in-fact authorized.

Enhancement 2

Interview

How does the alternate storage site support recovery operations? Are recovery times and recovery point objectives specified in the contingency plan? In the agreement with the site?

Examine

Review the contingency plan and the agreement with the alternate storage site to determine whether the organization configured the alternate storage site to facilitate recovery operations in accordance with the recovery time and recovery point objectives stated in the plan.

Enhancement 3

Interview

Has your organization identified potential accessibility problems to the alternate storage site in the event of an area wide disruption or disaster? Have mitigation actions been addressed in the contingency plan?

Examine

Review the contingency plan and the agreement with the alternate storage site to determine whether:

- The organization identified potential accessibility problems to the alternate storage site in the event of an area wide disruption or disaster.
- The organization addressed mitigation actions in the contingency plan.

B.7.6 CP-7 ALTERNATE PROCESSING SITE

Interview

Has your organization identified an alternate processing site? If so, have agreements been established to permit the transfer and assumption of essential mission and business functions at the site?

Are any equipment and supplies required to transfer and resume operations in place and available at the alternate processing site? If not, are contracts in place to support delivery to the site within the stated timeframe for transferring and assuming functions at the site?

What information security safeguards are provided at the alternate processing site? Are they documented in the agreement?

Examine

If the organization has established an alternate processing site, review the agreement established with the site to determine

- Whether the agreement supports the transfer and resumption of NRC defined system operations for essential missions/business functions within the NRC defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.
- Whether the agreement states that the equipment and supplies required to transfer and resume operations at the alternate processing site are available.
- Whether information security safeguards are documented in the agreement.
- Whether the safeguards are equivalent to that of the primary site.

Review contracts in place supporting delivery of equipment and supplies to the alternate processing site within the NRC defined time period for transfer/resumption.

Enhancement 1

Interview

Where is the alternate site located?

Examine

Review the contingency plan and the agreement with the alternate processing site to determine whether the site is located at a distance sufficient from the primary site to reduce susceptibility to the same threats.

Enhancement 2

Interview

Has your organization identified potential accessibility problems to the alternate storage site in the event of an area wide disruption or disaster? Have mitigation actions been addressed in the contingency plan?

Examine

Review the contingency plan and the agreement with the alternate processing site to determine whether organization identifies potential accessibility problems to the alternate processing site in the event of an area wide disruption or disaster and outlines explicit mitigation actions.

Enhancement 3

Interview

Does your organization have an agreement with the alternate processing site that provides priority of service provisions? What are the provisions?

Examine

Review the agreement with the alternate processing site to determine whether the agreements contain priority of service provisions in accordance with organizational availability requirements (including recovery time objectives).

Enhancement 4

Interview

What has your organization done to prepare the alternate processing site to be used as the operational site supporting essential missions and business functions?

Examine

Review the contingency plan and all organization documentation supporting transition to the alternate processing site to determine whether the site would be ready to be used as the operational site supporting essential missions and business functions.

B.7.7 CP-8 TELECOMMUNICATIONS SERVICES

Interview

Has the organization identified an alternate telecommunications service (data and voice) to support the system?

What is the alternate telecommunications service? Which carrier provides the telecommunication service?

What is the time period within which resumption of system operations must take place?

Is a service agreement in place to permit the resumption of telecommunications service for critical mission/business functions within the time period when the primary telecommunications capabilities are unavailable?

Examine

Review the contingency plan to determine whether the organization has established alternate telecommunications services including necessary agreements to permit the resumption of NRC defined system operations for essential missions and business functions within the NRC defined time period if the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Review agreements supporting alternate telecommunications services to determine whether the agreement states that the services will be provided within the NRC defined time period.

Enhancement 1

Interview

Are telecommunications services supporting your organization used for national security emergency preparedness?

Can your organization request Telecommunications Service Priority (TSP) for telecommunications services?

Does your organization have procedures that define how to request Telecommunications Service Priority? Where are the procedures defined?

Examine

Review the contingency plan and telecommunication service agreements to determine:

- Whether the organization has established agreements for primary and secondary alternate telecommunication services.
- Whether the agreements contain priority of service provisions in accordance with organizational availability requirements (including recovery time objectives).
- Whether the agreements state that Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness will be provided in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Enhancements 2, 3

Interview

Has the organization identified an alternate telecommunications service in the event that the primary service is not available?

What is the alternate telecommunications service? Which carrier provides the telecommunication service?

Is a service agreement in place with the alternate carrier?

Examine

Review the contingency plan and telecommunication service agreements to determine whether the organization:

- Obtained alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
- Obtained alternate telecommunications services from providers that are separated from the primary service providers to reduce susceptibility to the same threats.

Enhancement 4

Interview

Do the primary and alternate telecommunications service providers have contingency plans? If so, do you have copies of the plans?

How often does your organization review the plans? What do you look for during the course of the review?

How often do the service providers test the contingency plans? Does your organization receive copies of the test results?

How often do the service providers conduct contingency training? Does your organization receive evidence that training took place?

Examine

Review the contingency plan and telecommunication service agreements to determine whether the organization requires primary and alternate telecommunications service providers to have contingency plans.

Examine organization records to determine whether:

- The organization reviewed the provider contingency plans to ensure that the plans meet organizational contingency requirements.
- The organization obtained evidence of contingency testing/training by providers at the NRC defined frequency.

B.7.8 CP-9 SYSTEM BACKUP

Interview

How often does your organization backup user level information contained in the system?

How often does your organization backup system documentation, including security related documentation?

Where are system backups stored?

How does your organization protect the confidentiality, integrity, and availability of backup information at the storage locations?

Examine

Review organization backup plans and procedures to determine whether the organization:

- Conducts backups of user level information and system level information contained in the system at the NRC defined frequency consistent with recovery time and recovery point objectives.
- Conducts backups of system documentation including security related documentation at the NRC defined frequency consistent with recovery time and recovery point objectives.
- Protects the confidentiality, integrity, and availability of backup information at storage locations.

Test

Work with the ISSO and/or system administrator staff as required to define arrange and complete a test run of the applicable backup procedures. Observe this test use of system backup media to verify the organization successfully backs up user level information, system level information, and system documentation in accordance with NRC defined requirements.

Observe the mechanisms used to protect backup information to ensure that the backup mechanisms and methods adequately protect the confidentiality, integrity, and availability of backup information.

Inspect the backup media and files as necessary to verify that cryptography mechanisms used to protect backup information to ensure that they are FIPS-140-2 validated.

Enhancement 1

Interview

Does your organization test the backup information to verify that the media is reliable and the integrity of the information? If so, how often?

Examine

Review organization backup plans, procedures, and logs to determine whether the organization tests the backup information to verify that the media is reliable and the integrity of the information at the NRC defined frequency.

Test

Review documentation that provides evidence that backup media gets tested to verify media reliability and information integrity in accordance with NRC defined requirements.

Work with the ISSO and/or system administrator staff to arrange and complete a test restore of the applicable backup media and data using the system’s current recovery procedures.

Observe the test restore process and inspect the results for any errors to verify the organization can successfully recover their: user level information, system level information, and system documentation in accordance with NRC defined requirements.

Enhancement 2

Interview

Does your organization use backup information to restore selected system functions during contingency plan testing? If so, were the functions restored successfully?

Examine

Review the contingency plan, contingency test plan, and contingency test reports to determine whether the organization uses backup information to restore selected system functions during contingency plan testing, and to determine whether the functions were restored successfully.

Test

Inspect the storage location of backup media, if possible, to ensure that the organization does in-fact store NRC defined critical information in a separate facility or in a fire rated container that is not collocated with the operational system.

Enhancement 3

Interview

Where does your organization store backup copies of critical system software and security related information? What does your organization consider to be critical system software? Security related information?

Examine

Review organization backup plans, procedures, and logs to determine whether the organization stores backup copies of critical system software and other security related information in a separate facility or in a fire rated container that is not collocated with the operational system.

Test

Inspect the storage location of backup media, if possible, to ensure that the organization stores NRC defined critical information in a separate facility or in a fire rated container that is not collocated with the operational system, and to verify that backup media security procedures are followed to ensure the correct backup media will be there to support recovery if required and are appropriately protected.

Enhancement 5

Interview

How often does your organization transfer backup information to the alternate storage site? How is the backup transferred (electronically or physically)?

Examine

Review organization backup plans, procedures, and logs to determine whether the organization transfers backup information to the alternate storage site at the NRC defined frequency consistent with recovery time and recovery point objectives.

Review a sample of records that provide evidence that backup media are transferred to the alternate storage site in accordance with NRC defined requirements. These records must specify, at a minimum, the name of the individual(s) responsible for overseeing the transfer and the date and time the backup information was picked up for transfer.

<u>Test</u>

Work with the ISSO and system administrator staff to arrange for a literal test transfer of test or live backup information to the separate backup site. Observe and document the transfer procedures and whether the transfer method and data delivery is successful. For electronic transfers, verify the required data was transferred and without errors requiring a resend.

B.7.9 CP-10 SYSTEM RECOVERY AND RECONSTITUTION

<u>Interview</u>

Does your organization have mechanisms and procedures for recovery and reconstitution of the system to known secure state after disruption or failure? If so, what are the mechanisms and how do they support the recovery and reconstitution of the system?

Does the system contingency plan address the full recovery and reconstitution of the system? If so, which test in the plan addresses a full recovery and reconstitution?

<u>Examine</u>

Review the contingency plan, and organization recovery plans and procedures to determine:

- Whether the plans and procedures support the recovery and reconstitution of the system to a known secure state after disruption or failure.
- Whether the organization uses mechanisms to support the recovery and reconstitution of the system.
- Whether the system contingency plan addresses the full recovery and reconstitution of the system, and provides a test that addresses full recovery and reconstitution.
- Review the results of previous contingency tests to ensure that the system is able to successfully recover to a known secure state after disruption or failure.

<u>Test</u>

Work with the ISSO and system administrator staff to arrange for a literal test recovery of the system and its data, observing the procedures and mechanisms used for system recovery and reconstitution, as well as the testing used after recovery (i.e., scans, data integrity and compare checks, configuration scans or audits) to ensure the system is able to recover to its known and approved secure state after disruption or failure.

Observe the use of the recovery procedures and mechanisms verifying they perform successfully and adequately support recovery as intended. Document any failures and/or workarounds that may be required to complete the recovery.

<u>Enhancement 2</u>

<u>Interview</u>

Is the system transaction based? What is the nature of the transactions?

What mechanisms does your organization use to support transaction recovery?

Examine

If the system is transaction based, review the contingency plan and organization recovery plans and procedures to determine whether the organization uses mechanisms to support transaction recovery.

Test

If the system is transaction based, work with the ISSO and system administrator using a non-production instance of the same system to attempt some example recoveries of past transactions within the designed limits of the system. Observe the operation of the transaction recovery mechanisms to verify that the system logs all transactions and is able to successfully provide transaction recovery.

Enhancement 4

Interview

How has your organization captured the system's operational state? Does the state include appropriate system parameters, patches, configuration settings, and application/system software prior to system disruption or failure?

How long would it take to restore system components to an operational state?

Examine

Review the contingency plan and organization recovery plans and procedures to determine whether the organization provides the capability to restore system components within the NRC defined restoration time period from configuration controlled and integrity protected information representing a known, operational state for the components.

Test

Work with the ISSO and system administrator to execute a test recovery using the mechanisms intended to restore system components from configuration controlled and integrity protected system state backup information representing a known, operational state for the component, such as a recovery image, within NRC defined time periods.

B.8 IDENTIFICATION AND AUTHENTICATION (IA)

Identification and authentication assessment objects include, but are not limited to: policy and procedures; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; and tasks performed by organization staff in support of identification and authentication functions.

B.8.1 IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Interview

Are system-specific identification and authentication policies and procedures available?

Who is responsible for reviewing, updating, and disseminating these procedures?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated identification and authentication controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific identification and authentication policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.8.2 IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Interview

How does the system uniquely identify and authenticate users?

Are privileged users required to use PIV credentials for authentication? What percentage are not required?

Are non-privileged users required to use PIV credentials for authentication? What percentage are not required?

Does the system have any processes acting on behalf of users that require authentication? If so, please describe the processes.

Does your organization use group authenticators? If so, how are users uniquely identified within the groups?

Is the system accessible by the public?

Has an e Authentication Risk Assessment been conducted for the system in accordance with OMB M 04 04?

Where is the e Authentication Risk Assessment documented?

Are public users required to authenticate before gaining access to the system?

Examine

Review relevant system documentation to determine whether the organization uniquely identifies and authenticates organizational users (or processes acting on behalf of users), and to obtain an understanding of the organization's approach to identification and authentication.

Test

Work with the ISSO and system administrator and using NRC hands-on methods or approved tools for testing and auditing system identification and authentication methods, arrange for tool based testing of the accounts on the system. List and/or view the user accounts details and status present in the system. Verify that the system uniquely identifies and authenticates all users and, if applicable, system processes acting on behalf of users that require authentication. Verify there are no anonymous, guest, or shared accounts available that do not uniquely identify users.

Perform a test to determine the percentage of privileged and non-privileged users that are not required to use PIV credentials to logon.

Repeat the above test steps as necessary to verify what identification and authentication mechanisms, methods, modes and configurations (with the relevant encryption) are used for each interface to the system, including: Public or Internet facing (if applicable), intranet browser or client/thin client based, administrative and developer portals, etc.

Enhancements 1, 8

Interview

What level of authentication is required for network access to privileged accounts? What authentication method is used? Is the authentication mechanism replay resistant?

Examine

Review relevant system documentation to determine whether the organization implements multifactor authentication for network access to privileged accounts, and to determine the authentication mechanism used.

Test

Work with the ISSO and system administrator to observe a privileged user log onto the system using network access for privileged accounts to ensure that multifactor authentication is required, for each available interface. Observe the methods used. Note the properties or characteristics of the authentication method to verify that the mechanism complies with current NRC IA-policies and requirements. Verify that:

- The system requires multifactor authentication for network access to privileged (i.e., admin, developer, or super-user) accounts.
- The system requires replay resistant authentication (such as mechanisms that use cryptographic nonces or challenges and time synchronous or challenge response one time authenticators) for network access to privileged accounts.

Enhancements 2, 9

Interview

What level of authentication is required for network access to non-privileged accounts? What authentication method is used? Is the authentication mechanism replay resistant?

Examine

Review relevant system documentation to determine whether the organization implements multifactor authentication for network access to non-privileged accounts, and to determine the authentication mechanism used.

Test

Work with the ISSO and system administrator to observe a privileged user log onto the system using network access for non-privileged (i.e., standard) accounts to ensure that multifactor authentication is required. Observe the methods used. Note the properties or characteristics of the authentication method to verify the mechanism complies with current NRC IA-policies and requirements. Verify that:

- The system requires NRC requirements compliant multifactor authentication for network access to non-privileged (i.e., standard user, end-user) accounts.
- The system requires replay resistant authentication (such as mechanisms that use cryptographic nonces or challenges and time synchronous or challenge response one time authenticators) for network access to non-privileged accounts.

Enhancement 3

Interview

What level of authentication is required for local access to privileged accounts?

Examine

Review relevant system documentation to determine whether the organization implements multifactor authentication for local access to privileged accounts, and to determine the authentication mechanism used.

Test

Work with the ISSO and system administrator to observe a privileged user log onto the local system using a privileged account. Verify whether multifactor authentication is required. Observe and document the methods used. Note the properties or characteristics of the authentication method to verify that the mechanism complies with current NRC policies and requirements. Verify that:

- Identification and authentication mechanisms on the system require multifactor authentication for local access to privileged accounts.
- Arrange to observe a privileged user log onto the system locally to verify that multifactor authentication is required, that access without two factor is not provided.
- Work with the ISSO to arrange for test attempts to login with an expired or recently invalidated two-factor access card or token (i.e., for revoked user accounts) to confirm the user no longer has access to the system. Attempt to login with a revoked access card and observe the results. As the card is read and before the user would

be prompted to login the system should present a message stating the certificates, keys, or card is expired or invalid for access to the system. The user should not be provided an opportunity to login but should be referred to the appropriate officials.

- Test the system with a functional access card or token that can be locked out during testing. Attempt several logins with an invalid or guessed PIN or password. Observe that the system locks the access card and/or account as required.
- Work with the ISSO and system administrator to observe the staff follow the procedures necessary to unlock the test access card and/or user account to confirm the procedures are available, known, and accurate for the system. Do not however unlock any access cards, tokens, or accounts revoked by the agency for any other reasons.

Enhancement 4

Interview

What level of authentication is required for local access to non-privileged accounts?

Examine

Review relevant system documentation to determine whether the organization implements multifactor authentication for local access to non-privileged accounts, and to determine the authentication mechanism used.

Test

Review the configurations of identification and authentication mechanisms on the system to ensure that the system requires multifactor authentication for local access to non-privileged accounts.

If possible, observe a non-privileged user log onto the system locally to ensure that-multifactor authentication is required.

Enhancement 11

Interview

Is remote access to the system permitted? If so, are remote users identified and authenticated differently than local users?

Is multifactor authentication used? If so, does the authentication take place outside of the main system?

Examine

Review relevant system documentation to determine whether the organization implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets NRC defined strength of mechanism requirements.

Test

Review the configurations of identification and authentication mechanisms on the system to ensure that the system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets NRC defined strength of mechanism requirements.

Enhancement 12

Interview

Does the system accept and electronically verify PIV credentials?

Examine

Review relevant system documentation to determine whether the system accepts and electronically verifies PIV credentials.

Test

Review the configurations of identification and authentication mechanisms on the system to ensure that the system accepts and electronically verifies PIV credentials.

Observe a user log onto the system using PIV credentials to ensure that the system accepts these credentials.

B.8.3 IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Interview

Are system devices uniquely identified and authenticated before establishing:

- Local connections? If so, how?
- Remote connections? If so, how?
- Network connections? If so, how?
- Which devices are identified and authenticated?

Examine

Review relevant system documentation to determine whether the system uniquely identifies and authenticates NRC defined system devices before establishing local, remote, or network connections, and to obtain an understanding of the organization's approach to device identification and authentication.

Test

Arrange with the ISSO and system administrator team as needed to access or view the system's device identification and authentication mechanisms console or tools in operation. Work with the team to witness them attempt to remove and re-add both authorized devices and devices not yet authorized to connect to the system. Observe the mechanisms in operation to confirm that they do uniquely identify and authenticate NRC defined devices before establishing NRC defined types of connections, and that they successfully quarantine or reject unauthorized device connections.

B.8.4 IA-4 IDENTIFIER MANAGEMENT

Interview

Who authorizes your organization to assign individual, group, role, or device identifiers?

Who selects and assigns the identifiers?

How are the identifiers tracked to ensure that they are not reused?

How long after an identifier is inactive is the identifier disabled?

Examine

Examine organization records to determine whether the organization received authorization from the NRC defined personnel or role to assign individual, group, role, or device identifiers.

Review date and time stamped, system generated lists of individual, group, role, and device identifiers to determine:

- Whether the organization prevents reuse of identifiers for the NRC defined time period.
- Review a sample of access account history records that provide evidence confirming that a designated organizational official authorizes the use of each user or device identifier prior to the identifier being assigned.
- Whether identifiers are disabled after the NRC defined period of activity.

Test

Work with the ISSO and/or system administrator team as necessary to access and observe the system’s automated mechanisms (i.e., consoles or tools) supporting and/or implementing the system’s user or access account identifier management.

Inspect the configurations of identification management mechanisms to confirm that the organization manages the system’s user or access account identifiers (human or service accounts/other), including preventing the reuse of assigned identifiers and disabling inactive identifiers in accordance with NRC defined requirements.

Arrange with the ISSO and system administrator team as necessary to observe authorized system personnel walk-through or demonstrate how they follow NRC approved identifier management processes, such as creating a new identifier for a new user, maintaining only the authorized user identifiers on the system, and locking or disabling any access accounts that are no longer authorized.

B.8.5 IA-5 AUTHENTICATOR MANAGEMENT

Interview

How does your organization verify the identity of the individual, group, role, or device receiving an authenticator?

Has your organization defined initial authenticator content? If so, where is the content documented?

Do user and system authenticators (e.g., passwords) meet or exceed NRC requirements based on the system categorization?

Does your organization have administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and for revoking authenticators? If so, where are they documented?

How often does your organization change authenticators? Who is responsible for doing so? Where are the changes documented?

How does your organization protect authorization content from unauthorized disclosure and modification?

Does your organization require individuals to implement specific security safeguards to protect authenticators? If so, where are the required security safeguards documented?

How does your organization handle group/role authenticators when membership changes? Is this process documented?

Examine

Examine organization records to determine whether the organization:

- Verifies the identity of individuals, groups, roles, or devices during initial authenticator distribution.
- Establishes initial authenticator content for authenticators defined by the organization.
- Changes or refreshes authenticators at the NRC defined time period for the authenticator type.
- Changes authenticators for group/role accounts when membership to those accounts changes.

Review relevant system documentation to determine whether the organization:

- Ensures that authenticators have sufficient strength of mechanism for their intended use.
- Establishes and implements administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
- Changes the default content of authenticators before system installation.
- Establishes minimum and maximum lifetime restrictions and reuse conditions for authenticators.
- Protects authenticator content from unauthorized disclosure and modification.
- Requires individuals to take, and having devices implement, specific security safeguards to protect authenticators.

Test

Arrange with the ISSO and system administrator team as necessary to access and inspect the system’s authentication management mechanisms (i.e., Authentication, authorization, and accounting [AAA]) configurations to verify that the organizations automation and procedures allow it to manage the systems authenticators in accordance with NRC defined requirements, including those above.

Work with the ISSO and system administrator team to witness and observe authorized system personnel demonstrate their authenticator management processes, such as observing them verify the identity of a new user prior to issuing the user initial authenticator content (such as a temporary/initial passphrase) and carrying out NRC approved procedures for lost/compromised or damaged authenticators, passphrases, or certificate keys.

Request that the ISSO and/or system administrator team walk through the use of their automated authentication management mechanisms and manual procedures to confirm that the organization does define and implement NRC requirements and characteristics for initial authenticator content (i.e., password, passphrase, or key characteristics and the procedures for changing initial authenticator content).

Access and inspect the properties of the system's authentication management mechanisms configuration as implemented to ensure that authenticators have sufficient strength of mechanism (adequate encryption etc.) for their intended use, and no unacceptable methods are provided or allowed.

Scan each system interface with an NRC approved tool setup to test authentication mechanisms. Confirm the system does not use or allow any outdated or rejected encryption methods or strengths (i.e., NTLM, SSL2, DES, 56bit) for authentication.

Inspect the properties of the system's authentication management mechanisms to determine where authenticator content is stored on the system and ensure that the organization protects this authentication content from unauthorized disclosure and modification. View the list of accounts that have any access to the storage location of authentication content and confirm the accounts require access.

Inspect the configurations of authentication management mechanisms as implemented to confirm that devices implement specific security safeguards to protect stored or transmitted authenticators, such as appropriate access controls and adequate encryption.

Work with the system ISSO and/or system administrator as necessary to inspect authentication management mechanisms as used to verify that the organization changes authenticators for group/role (effectively shared if allowed) accounts when membership to those group accounts change. Locate a group/role account if present and determine when any user was last removed from the group or role, and if log information or records indicate that the role account authenticators were in fact changed following that event.

Enhancement 1

Interview

For password based authentication, how does the system protect passwords from unauthorized disclosure and modification when stored and transmitted?

Are temporary passwords assigned to a new user? If so, does the system force the user to change this temporary password before proceeding?

Examine

Review relevant system documentation to determine whether for password based authentication, the system:

- Enforces the NRC’s password complexity requirements.
- Stores and transmits only encrypted representations of passwords.
- Enforces NRC defined password minimum and maximum lifetime restrictions.
- Prohibits password reuse for the NRC defined number of generations.
- Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Test

Using NRC approved tools for auditing and testing system security hardening and configurations work with the ISSO and system administrator team to scan the system’s automated authentication management mechanism configurations to verify that for password based authentication, the system:

- Enforces the NRC’s password complexity requirements.
- Stores and transmits only adequately encrypted representations of passwords.
- Enforces NRC defined password minimum and maximum lifetime restrictions.
- Prohibits password reuse for the NRC defined number of generations.
- Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Enhancement 2

Interview

For Public Key Infrastructure (PKI)-based authentication, how are certifications validated? Is a local cache of revocation data maintained (to support path discovery and validation) in case revocation information can’t be accessed via the network?

Examine

Review relevant system documentation to determine whether for PKI-based authentication, the system:

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

Test

Work with the ISSO and system administrator team as needed to understand any PKI-based authentication mechanisms required and implemented for the system. Request the team login and walk through their automated authentication management mechanisms or consoles and their log information or records for PKI-based authentication, to verify that the system:

- Shows in the tools how it validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status (and revocation) data. Trust path and anchor configurations should be inspected and verified as valid. Confirm that authentication of users invokes the use of the appropriate trust anchors.
- Enforces authorized access to the corresponding private key, meaning that any private keys or private key files may only be read, copied, viewed, or accessed by authorized users requiring such access with NRC approved need-to-know. Inspect the list of users with access to the private key files or key rings on the system and confirm the access allowed is necessary and authorized by NRC defined policies.
- Maps authenticated identities only to the account of the correct individual or group.
- The automated mechanisms maintain a local cache of revocation data to support path discovery and user certificate or key validation in the event of any inability to access revocation information via the network.

Enhancement 3

Interview

How does an individual obtain authenticators? Is this process documented?

Examine

Review relevant system documentation to determine whether the organization has a formal registration process to receive NRC defined types of and/or specific authenticators using the NRC defined method (e.g., in person; or by a trusted third party) before the NRC defined registration authority with authorization by the NRC defined personnel.

Test

Arrange to have the ISSO and system administrator team’s authorized system personnel walk through and demonstrate how they perform the registration process for issuing new authenticators in accordance with NRC defined requirements.

Enhancement 11

Interview

Does your organization use NRC provided PIV cards for hardware token based authentication?

Examine

Review relevant system documentation to:

- Determine whether the organization, for hardware token based authentication, employs mechanisms that satisfy NRC defined token quality requirements.

- Obtain an understanding of the organization's approach to hardware token based authentication.

Test

Work with the ISSO and system administrator team as needed to walk through test runs of the system's hardware token based authentication mechanisms as applicable to verify the mechanisms are implemented and operate in accordance with NRC defined requirements.

B.8.6 IA-6 AUTHENTICATOR FEEDBACK

Interview

Does the system obscure authenticator feedback? If so, how?

Examine

Review relevant system documentation to determine whether authenticator feedback is obscured.

Test

Observe a user log onto the system, at each of the system's user and administrative interfaces, to ensure that when authenticators are entered, authenticator feedback is obscured.

B.8.7 IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Interview

Does the system authenticate to a cryptographic module? If so, is the module certified as FIPS-140-2 validated? Is a certificate available stating so?

Examine

Review relevant system documentation to determine whether the system 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.

Work with the ISSO and system administrator team to access and review the as-built implemented configurations of identification and authentication mechanisms on the system to ensure that the system is configured to accept and electronically verify PIV credentials.

Test

Work with the ISSO and system administrator team as needed to scan the system's authentication mechanisms for each interface with NRC approved security scanning tools covering both network and local access controls. Confirm that the scanner only identifies FIPS-140-2 validated cryptography in use for identification and authentication or findings in its implementation.

Observe a user log onto the system using NRC-compliant PIV credentials to ensure that the system accepts these credentials.

B.8.8 IA-8 IDENTIFICATION AND AUTHENTICATION (NON ORGANIZATIONAL USERS)

Interview

Does your organization permit non organizational users access to the system? If so, how are they identified and authenticated?

Examine

If the organization permits non organizational users access to the system, then review relevant system documentation to obtain an understanding of how they are identified and authenticated.

Inspect logs of non-organizational user access to determine whether they were identified and how, and to confirm they were authenticated as documented.

Test

Work with the ISSO and system administrator to obtain test non-organizational (such as public) user accounts to test identification and authentication management mechanisms for non-organizational users (or processes acting on behalf of non-organizational users) that require authentication. If that is not possible arrange to observe a sampling of non-organizational (i.e., public, partner, vendor) users logging into their accounts on the system.

Observe the non-organizational users log onto the system and note what types of authentication is required, how it functions, and any authentication properties identifiable during testing to verify that NRC-defined requirements are met.

Enhancement 1

Interview

Does the system accept and electronically verify PIV credentials from other federal agencies?

Examine

Review relevant system documentation to determine whether the system accepts and electronically verifies PIV credentials from other federal agencies.

Review the configurations of identification and authentication mechanisms on the system to ensure that the system accepts and electronically verifies PIV credentials from other federal agencies.

Test

Arrange with the ISSO and system administrator as needed to have a sampling of users from another federal agency log onto the system using PIV credentials from another federal agency to verify that the system accepts these credentials; or if none are available for the test cycle the team may access and inspect the system authentication logs and account database for records proving how the system does in fact authenticate PIV users from other federal agencies.

Enhancements 2, 3, 4

Interview

Public facing Websites: Does the system require FICAM approved third party credentials? Are all system components that are used to accept the credentials FICAM approved? Does your system conform to FICAM issued profiles?

Examine

For systems accessible to the general public, such as public facing websites, Review relevant system documentation to determine:

- Whether the system requires and accepts only FICAM approved third party credentials.
- Whether all system components that are used to accept the credentials are FICAM approved.
- Whether the system conforms to FICAM issued profiles. The current list of FICAM approved [id]management.gov I&A products are listed at the URL: http://www.idmanagement.gov/approved-products-list.

Test

For systems accessible to the general public, such as public facing websites, using live test or sample access accounts known to be FICAM compliant login to the systems web-facing identification and authentication mechanisms, and inspect the system or application logs after the authentication succeeds to verify that:

- System components successfully accept FICAM approved credentials.
- The system's automated identification and authentication components are FICAM approved.
- The system's automated mechanisms conform to FICAM issued profiles. The system or applications event logs should indicate the FICAM-based user login was successful with no significant errors indicating failures of FICAM methods.
- Working with the ISSO and system team access and verify that the properties of the system's implemented automated mechanisms used to provide FICAM approved access verify accurately against the official list of FICAM approved products, and as per NRC-defined requirements.

B.9 INCIDENT RESPONSE (IR)

Incident response assessment objects include, but are not limited to: policy and procedures; incident response plans; incident response test plans and incident response test reports; records of actual security incidents; and tasks performed by organization staff in support of incident response functions.

B.9.1 IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

<u>Interview</u>

Are system-specific incident response procedures available?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that these reviews and updates took place?

<u>Examine</u>

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated incident response controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific incident response policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.9.2 IR-2 INCIDENT RESPONSE TRAINING

<u>Interview</u>

Does your organization conduct incident response training? If so, how often does training take place? Are there records to support that training took place, and who was trained during each session?

<u>Examine</u>

<u>Examine</u> organization records to determine whether:

- The organization provides incident response training to system users consistent with assigned roles and responsibilities.

- Training is provided within the NRC defined timeframe of assuming an incident response role or responsibility.
- Training is provided when required by system changes.
- After initial training, the organization provides training at the NRC defined frequency.

Enhancement 1

Interview

Does your organization include simulated events and scenarios in incident response training? If so, where are the events and scenarios documented?

Examine

Review training materials to determine whether the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Test

Request the NRC team or contractors that provide NRC incident response training carry out a walk-through or demo of any automated mechanisms (software or tools etc.) used to provide simulated events for incident response training. Verify the training simulation is able to assist personnel in understanding and providing effective response in crisis situations that might impact the NRC. Check if the automation is able to assess teams tested using the simulation and the results. Personnel may be surveyed for feedback.

Enhancement 2

Interview

Does your organization use automated mechanisms during incident response training? If so, what are the mechanisms, and how are they used during training?

Examine

Review system incident response documentation to determine whether the organization employs automated mechanisms to provide a more thorough and realistic training environment (such as simulated realistic events) during incident response training.

Test

Request the NRC team or contractors that provide NRC incident response training carry out a walk-through or demo of any automated mechanisms (software or tools etc.) used to provide simulated events for incident response training. Verify the training simulation is able to provide a more thorough and realistic incident response training environment with situations that may impact the NRC. Personnel may be surveyed for feedback.

B.9.3 IR-3 INCIDENT RESPONSE TESTING

Interview

Does your organization conduct incident response testing? If so, how often does testing take place? Are test results documented? If so, where?

Examine

Review all historical incident response test plans and test reports to determine whether the organization in-fact tests the incident response capability for the system:

- at the NRC defined frequency, and
- Using NRC defined tests to determine the effectiveness of the incident response capability, including capabilities that may be handled by third parties for the NRC.
- The incident response test plans provide adequate scope coverage of the NRC-defined required IR-testing objectives, using adequate methods, tools, and reporting.

Enhancement 2

Interview

Does your organization coordinate incident response testing with other organizations responsible for related plans? If so, which organizations, and which plans?

Examine

Examine organization records to determine whether the organization did coordinate incident response testing with other organizations responsible for related plans and when they have any control of or stake or responsibilities for the system.

If possible, review incident response test reports for the other organizations to determine whether the reports indicate that coordination took place.

B.9.4 IR-4 INCIDENT HANDLING

Interview

How does your organization handle incidents? Are lessons learned during the incidents documented? If so, where?

Examine

Review relevant system documentation to determine whether the organization:

- 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. Were meetings held to discuss lessons learned?
- Records of how the team handled a sampling of past actual security incidents to determine whether the incidents were handled as documented in the systems IR-plan documentation and in accordance with NRC defined policy

- Effectively includes and obligates any external contractors or 3rd party stakeholders with responsibilities over the system operations or its data to support the incident handling process, as per NRC-defined policies.

Test

Arrange with the ISSO and system stakeholders identified in their incident response plan to walk through and exercise their security incident response handling capabilities. A simulated system security breach or policy violation could be used with the team walking through a test response using their IR-procedures and incident handling capabilities. The test scenario used should be adequate to confirm that the organization may respond to a breach or incident effectively in accordance with NRC defined policy.

Enhancement 1

Systems Hosted in Non NRC Facilities:

Interview

Does your organization use automated mechanisms to support the incident handling process? If so, what are the mechanisms, and how are they used?

Examine

Review system incident response documentation to determine whether the organization employs automated mechanisms to support the incident handling process.

Examine records of actual past security incidents to determine whether automated mechanisms were used effectively to support the incident handling process.

Test

Arrange with the ISSO and system stakeholders identified in their incident response plan to exercise and trigger their automated security incident response handling capabilities. Arrange for and observe an agreed upon simulated system security breach or policy violation event and the system team's response (including 3rd party team members) while using their IR-procedures and incident handling capabilities. Confirm the automated mechanisms support the incident handling process. The test scenario used should be adequate to confirm that the organization may respond to a breach or incident effectively in accordance with NRC defined policy.

Enhancement 4

Systems Hosted in Non NRC Facilities:

Interview

Does your organization correlate incident information and individual incident responses to achieve an organization wide perspective on incident awareness and response?

Examine

Review system incident response documentation to determine whether the organization correlates incident information and individual incident responses to achieve an organization wide perspective on incident awareness and response.

Examine records of actual security incidents to determine whether the records correlate incident information and individual incident responses to achieve an organization wide perspective on incident awareness and response.

Test

Arrange with the ISSO and 3rd party stakeholders identified in the incident response plan and/or SLA or MOU or contract to exercise and trigger their automated security incident response handling capabilities, or manual incident handling processes. Arrange for and observe an agreed upon simulated system security breach or policy violation event and the system team's response (including 3rd party team members) while using their IR-procedures and incident handling capabilities. Confirm any automated mechanisms support the incident handling process. The test scenario used should be adequate to confirm that the organization may respond to a breach or incident effectively in accordance with NRC defined policy.

B.9.5 IR-5 INCIDENT MONITORING

Interview

Does your organization document all security incidents? If so, where are they documented? Who are the incidents reported to?

Examine

Review system incident response documentation to determine whether the organization tracks and documents system security incidents.

Review records that document the details of prior system security incidents that have occurred on the system to ensure that the organization tracks and documents system security incidents.

Test

Work with the ISSO and system team request a demonstration or live test of their incident monitoring and reporting capabilities the organization uses (manual and/or automated) to assist in the tracking of security incidents as well as the collection and analysis of security incident information. A practice exercise or security incident should be used to exercise the capabilities. Verify that the team has been using the capabilities and mechanisms to in fact document and report security incidents as expected, and is prepared to do so as required by NRC policies. Use any console or methods provided to confirm records of past incidents and their reporting.

Enhancement 1

Systems Hosted in Non NRC Facilities:

Interview

Does your organization use automated mechanisms to track security incidents and capture related data? If so, what are the mechanisms, and how are they used?

Examine

Review system incident response documentation to determine whether the organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Test

Work with the ISSO and system team request and observe a demonstration or live test of their automated incident monitoring and reporting capabilities used to assist in the tracking of security incidents as well as the collection and analysis of security incident information. A practice exercise or security incident event should be used to exercise the automation. Based on the events of the exercise or test scenario verify that the automated mechanisms in fact capture and document security incidents as required by NRC policies. Use any console or tools provided by the automation to evaluate and confirm records of selected incidents, the data collected, and its handling.

B.9.6 IR-6 INCIDENT REPORTING

Interview

Does your organization report all security incidents? If so, within what timeframe and how? Who are the incidents reported to?

Examine

Review system incident response documentation to determine whether the required timeframe and recipient of the incident report are identified.

Review records that document the details of incident reporting to ensure that the organization appropriately reports system security incidents.

Test

Work with the ISSO and system team request a demonstration or live test of their incident monitoring and reporting capabilities the organization uses (manual and/or automated) to assist in the tracking of security incidents as well as the collection and analysis of security incident information. A practice exercise or security incident should be used to exercise the capabilities. Verify that the team has been using the capabilities and mechanisms to in fact document and report security incidents as expected, and is prepared to do so as required by NRC policies. Use any console or methods provided to confirm records of past incidents and their reporting.

Enhancement 1

Automated reporting:

Interview

Does your organization use automated mechanisms to report security incidents and capture related data? If so, what are the mechanisms, and how are they used?

Examine

Review system incident response documentation to determine whether the organization employs automated mechanisms to assist in the reporting of security incidents and in the collection and analysis of incident information.

Test

Work with the ISSO and system team request and observe a demonstration or live test of their automated incident monitoring and reporting capabilities used to assist in the tracking of security incidents as well as the collection and analysis of security incident information. A practice exercise or security incident event should be used to exercise the automation. Based on the events of the exercise or test scenario verify that the automated mechanisms in fact capture and document security incidents as required by NRC policies. Use any console or tools provided by the automation to evaluate and confirm records of selected incidents, the data collected, and its handling.

B.9.7 IR-7 INCIDENT RESPONSE ASSISTANCE

Interview

Does your organization provide user incident response assistance? If so, who provides it and how? Is assistance offered or must the user request it?

Examine

Review system incident response documentation to determine whether the organization tracks and documents incident response assistance.

Test

Work with the ISSO and system team request a demonstration or live test of their incident monitoring and reporting capabilities the organization uses (manual and/or automated) to witness user incident response assistance. A practice exercise or security incident should be used to exercise the capabilities. Verify that the team provides user incident response assistance. Use any console or methods provided to confirm records of past incidents and any assistance provided.

Enhancement 1

Automated mechanisms to increase the availability of incident response-related information and support:

Interview

Does your organization use automated mechanisms to increase the availability of incident response-related information and support? If so, what are the mechanisms, and how are they used?

Examine

Review system incident response documentation to determine whether the organization employs automated mechanisms to increase the availability of incident response-related information and support.

Test

Work with the ISSO and system team request and observe a demonstration or live test of their automated incident monitoring and reporting capabilities used to increase the availability of incident response-related information and support. A practice exercise or security incident event should be used to exercise the automation. Based on the events of the exercise or test scenario verify that the automated mechanisms in fact capture and document security incidents as required by NRC policies. Use any console or tools provided by the automation to evaluate and confirm use of the automated mechanisms to increase the availability of incident response-related information and support.

B.9.8 IR-8 INCIDENT RESPONSE PLAN

Interview

Does your organization have an Incident Response Plan?

Has the Incident Response Plan been reviewed and approved by designated organizational officials?

Who is responsible for reviewing and approving the plan? Are there records to support that the review and approvals have occurred?

Were incident handling activities coordinated with contingency planning activities? If so, how?

Examine

Review the incident response plan to determine whether the plan:

- 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;
- Is reviewed and approved by NRC defined personnel (or roles); and
- Is reviewed and updated by the organization at the NRC defined frequency or to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Examine organization records to determine whether:

- The plan was distributed to NRC defined key contingency personnel and organizational elements.
- The organization communicated changes to the plan to NRC defined key contingency personnel and organizational elements.

Review the incident response plan to determine whether the plan is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, "System Artifact Examination Procedure."

Test

Work with the ISSO and system team as necessary to attempt access to the team's incident response plan(s). Inspect the IR-plan storage location and folder/file security and the access accounts given permission to it to determine what accounts are allowed to view, use, or access the file. Note which accounts have "super-user" rights to delete or change the plan. Verify with the system team if these access rights are current and appropriate and under an NRC approved need to know. Verify that no access accounts possess excessive rights or permissions to delete the plan or to change it.

B.10 MAINTENANCE (MA)

Maintenance assessment objects include, but are not limited to: policy and procedures; records of actual system maintenance; vendor maintenance or support agreements; and tasks performed by organization staff in support of maintenance functions.

B.10.1 MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Interview

Are system-specific system maintenance procedures available?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated system maintenance controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific system maintenance policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.10.2 MA-2 CONTROLLED MAINTENANCE

Interview

Who is responsible for scheduling and reviewing records of routine preventative and regular maintenance?

Are there records to support that these reviews and updates took place?

Who is responsible for performing routine preventative and regular maintenance? Is the maintenance documented? If so, where, and who is responsible for documenting the performed maintenance? Please provide the maintenance records for review.

How does your organization ensure that maintenance performed on system components is in accordance with manufacturer or vendor specifications and/or organizational requirements?

What steps are taken to ensure that maintenance activities, including routine, scheduled maintenance and repairs are approved and controlled?

Who is responsible for approving and controlling maintenance activities?

What is the process for tracking equipment removed to another location for maintenance or repairs?

Who approves the removal of the system or system components from the facility when offsite maintenance or repairs are necessary? Where is the approval documented?

Are there procedures for removing information from associated media before removing equipment from the facility?

After maintenance is performed on the system, what checks are performed to verify that the security controls are still functioning properly?

Examine

Review system maintenance documentation to determine whether the organization:

- Schedules, performs, documents, and reviews records of maintenance and repairs on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

- Requires that NRC defined personnel explicitly approve the removal of the system or system components from organizational facilities for offsite maintenance or repairs;
- Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for offsite maintenance or repairs;
- Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
- Includes the NRC defined information in organizational maintenance records.

Examine records of actual system maintenance to verify that the organization performs and documents system maintenance activities as documented in system maintenance documentation and in accordance with NRC defined requirements.

Enhancement 2

Interview

Does your organization use automated mechanisms to schedule, conduct, and document maintenance and repairs? If so, what are the mechanisms, and how are they used? Please provide a current maintenance report detailing all repair and maintenance activities.

Examine

Review system maintenance documentation to determine whether the organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs.

Test

Work with the system ISSO and system administrator team to access and observe any automated mechanisms used to schedule, conduct, and document maintenance and repairs activities to verify that maintenance records for all requested, scheduled, in process, and completed maintenance activities are up to date, accurate, and complete.

B.10.3 MA-3 MAINTENANCE TOOLS

Interview

Who is responsible for approving, controlling, and monitoring the use of system maintenance tools?

How do they approve, control, and monitor the use of system maintenance tools? Is this process documented?

Who maintains the maintenance tools?

How are the tools maintained on an ongoing basis?

Are there records of approvals and tool maintenance?

Examine

Review system maintenance documentation to determine whether organization approves, controls, and monitors system maintenance tools.

Examine records of actual system maintenance to verify that the organization approves, controls, and monitors system maintenance tools.

Enhancement 1

Interview

Are maintenance tools inspected before being carried into a facility by maintenance personnel for obvious improper modifications?

Who conducts the inspections? Are results of the inspections documented? If so, where?

Do the individuals who conduct the inspections have the technical expertise to recognize improper maintenance tools and to recognize potential improper use of proper maintenance tools?

Examine

Review system maintenance documentation to determine whether the organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Examine records of actual system maintenance to verify that the organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Enhancement 2

Interview

Have media with diagnostic test programs been tested for malicious code before the media is used in the system? Have the tests been documented?

Who is responsible for testing media for malicious code?

What is the procedure for testing media for malicious code? Is the procedure documented? If so, where?

Examine

Review system maintenance documentation to determine whether the organization checks media containing diagnostic and test programs for malicious code before the media are used in the system.

Examine records of actual system maintenance to verify that the organization checks media containing diagnostic and test programs for malicious code before the media are used in the system.

Test

Arrange with the ISSO and system administrator team to gather and inspect a random sampling of system maintenance tools or media already on the site. Scan the media for malicious code, noting the results.

Next, work with the system team to walk through their current process for bringing in new maintenance media and testing it for malicious code and malware per the NRC-defined requirements. Verify that the organizational processes and any automated mechanisms used for inspecting maintenance media for malware or malicious code are effective and meet NRC-defined requirements.

Enhancement 3

Interview

How does your organization prevent the unauthorized removal of maintenance equipment containing organizational information? Is this procedure documented? If so, where?

Who is responsible for ensuring that maintenance equipment does not contain organizational information?

Who issues exemptions explicitly authorizing removal of the equipment from the facility?

Examine

Review system maintenance documentation to determine whether the organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

- Verifying that there is no organizational information contained on the equipment;
- Sanitizing or destroying the equipment;
- Retaining the equipment within the facility; or
- Obtaining an exemption from NRC defined personnel explicitly authorizing removal of the equipment from the facility.

Examine records of actual system maintenance to verify that the organization prevents the unauthorized removal of maintenance equipment containing organizational information as documented in system maintenance documentation and in accordance with NRC defined requirements.

B.10.4 MA-4 NON-LOCAL MAINTENANCE

Interview

Who is responsible for authorizing, monitoring, and controlling remotely executed maintenance and diagnostic activities?

How are remotely executed maintenance and diagnostic activities authorized?

How are remotely executed maintenance and diagnostic activities monitored?

How are remotely executed maintenance and diagnostic activities controlled?

Are there records for all remote maintenance and diagnostic activities?

Is all remote maintenance conducted exclusively via the internet or other external, non NRC network?

Examine

Review system maintenance documentation to determine whether the organization:

- Approves and monitors non-local maintenance and diagnostic activities;
- Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
- Employs strong authenticators in the establishment of non-local maintenance and diagnostic sessions;
- Maintains records for non-local maintenance and diagnostic activities; and
- Terminates session and network connections when non-local maintenance is completed.

Examine records of actual system maintenance to verify that the organization approves, monitors, and documents non-local maintenance activities as documented in system maintenance documentation and in accordance with NRC defined requirements.

Test

Work with the ISSO and system team as necessary to understand and observe samples of the system's non-local maintenance activities, sessions and connections as well as the processes the team uses to manage these. If there are no active sessions request the team initiate one for test purposes if possible. Access and observe the properties of active non-local maintenance connections to verify that:

- The system's authentication mechanisms (automated or other) employ strong authenticators meeting NRC security requirements in the establishment of any non-local (or remote) maintenance and diagnostic sessions.
- Any automated mechanisms used for terminating non-local maintenance sessions and network connections are effective in the NRC-defined time period. Allow an active session to expire as a test and ensure it is terminated per NRC policies.

Work with the ISSO and system team as necessary to understand, access, and observe any automated mechanisms used to implement, support, and/or manage their systems non-local maintenance activities (if any) to verify that all non-local maintenance sessions are monitored, audited, and meet all applicable NRC-defined security requirements.

Enhancement 2

Interview

Does the SSP address the use of remote maintenance and diagnostic tools?

Examine

Review the SSP or other relevant documentation to determine whether the organization documents the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.

Enhancement 3

Interview

How does your organization ensure that organizational information is sanitized before non-local maintenance and diagnostic services are performed?

Are components removed from your facility inspected and sanitized on return to the facility, and before reconnecting the component to your system?

Examine

Review system maintenance documentation to determine whether the organization:

- Requires that non-local maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or
- Removes the component to be serviced from the system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the system.

Examine records of actual system maintenance to verify that the organization enforces comparable security* for non-local maintenance and/or sanitizes the component prior to removal from organization facilities as documented in system maintenance documentation and in accordance with NRC defined requirements.

*Testing to verify any external organization has implemented and maintains all necessary security controls to ensure comparable security may not be feasible in the scope of many assessments, unless that external organization must access NRC sensitive data.

Test

Work with the ISSO and system team to exercise or walk through the organizational processes and any automated mechanisms used to support or provide component sanitization (i.e., sanitize sensitive data) and inspection for sensitive data prior to non-local maintenance. Verify that the methods used do in fact successfully sanitize the devices as per NRC-defined sanitization policies to prevent leaks or loss of NRC sensitive data through non-local maintenance. – OR-

Work with the ISSO and system team to exercise their organizational processes (manual or other) for the removal, sanitization and inspection of components from the system that may contain any sensitive data before and after being serviced via non-local maintenance. Components that may not be sanitized should be removed to protect NRC sensitive data.

Work with the ISSO and system team to test the processes used to scan and inspect components after non-local maintenance to ensure the components are also sanitized of any malware or malicious code potentially encountered by the device or component during maintenance and before it may be reconnected to the system. Verify that the processes and measures sanitize the devices per NRC requirements.

B.10.5 MA-5 MAINTENANCE PERSONNEL

Interview

Are only authorized personnel allowed to perform maintenance on the system? Is a list maintained of authorized maintenance organizations and personnel?

Do these personnel have the appropriate access authorizations to the system and its information?

Is there a process for authorizing maintenance personnel? If so, is it documented?

Are maintenance personnel without proper access authorizations supervised by personnel with proper access authorizations and technical competence during the performance of maintenance activities on the system?

Examine

Review system maintenance documentation to determine whether the organization:

Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

Ensures that non-escorted personnel performing maintenance on the system have required access authorizations; and

Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Test

Arrange a walk-through test to observe and verify the effectiveness of the processes used by the organization for authorizing and managing system maintenance personnel access records and escorting needs with the ISSO or system admins, including test use of any automated mechanisms used to support and/or implement authorization of maintenance personnel per NRC policies, carrying out test runs of administrative actions such as:

- Verifying the identity of a new maintenance user and creating a new maintenance access account and/or site access control list assignments.
- Maintaining, verifying, and updating any system maintenance access control lists used to authorize access for maintenance personnel as access needs change. Verify that these processes ensure only authorized users remain on access control lists used to authorize access to the system or its data.
- Verifying what system access rights and permissions maintenance personnel will require and granting / controlling access based on NRC approved job duty assignments and legitimate need-to-know.
- Verifying how the system team carries out escort and supervision procedures for maintenance personnel who do not possess NRC access authorizations in order to meet all NRC-defined security requirements for visiting maintenance personnel.

Enhancement 1

Interview

Does your organization have procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens? If so, where are the procedures documented?

Are the maintenance personnel escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified?

Are all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured before maintenance and diagnostic activities are conducted?

Does your organization implement alternate security safeguards in the event that a system component cannot be sanitized, removed, or disconnected from the system? Are the safeguards documented?

Examine

Review system maintenance documentation to determine whether the organization:

- Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens; and
- Develops and implements alternate security safeguards in the event a system component cannot be sanitized, removed, or disconnected from the system.

Test

Work with the ISSO and system team as necessary to arrange for a walk-through test of organizational processes used for managing maintenance personnel without appropriate access to verify that the processes meet all NRC-defined security requirements for personnel performing maintenance on the system are met; -OR-

Work with the ISSO and system team to test and verify the successful operation of any automated mechanisms supporting and/or implementing information storage component sanitization used to purge any NRC sensitive data as per NRC-defined requirements prior to any maintenance being performed by personnel who do not possess the required access clearance or authorizations.

B.10.6 MA-6 TIMELY MAINTENANCE

Interview

Who is responsible for ensuring that maintenance support and/or spare parts for key components identified in the Business Impact Assessment (BIA) are obtained?

Per your maintenance or support agreement, how long may it take to obtain support or spare parts? Is a copy of the maintenance agreement available for review?

Examine

Review vendor maintenance agreements or other relevant system maintenance documentation to determine whether the organization obtains maintenance support and/or spare parts for NRC defined system components within the NRC defined time period of failure.

B.11 MEDIA-PROTECTION (MP)

Media protection assessment objects include, but are not limited to: policy and procedures; actual system media and media storage mechanisms; records of media transport; and tasks performed by organization staff in support of media protection functions.

B.11.1 MP-1 MEDIA-PROTECTION POLICY AND PROCEDURES

Interview

Are system-specific media protection procedures available?

Have the specific measures used to protect the selected media and information contained on that media been defined in the procedures?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated media protection controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific media protection policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.11.2 MP-2 MEDIA-ACCESS

Interview

How is access restricted to digital and non-digital media to authorized individuals?

Examine

Review media protection documentation to determine whether the organization restricts access to NRC defined types of digital and non-digital media to NRC defined personnel.

Observe the storage location and access enforcement mechanisms for system media to ensure that the organization restricts access to system media in accordance with NRC defined requirements.

Test

Working with the system team and a small sample of system media ask the system personnel to demonstrate the organizational processes and controls that are used for restricting information media access to authorized individuals only, including automated mechanisms. Attempt to use or browse to some of the sample media to verify that the controls prevent unauthorized access to the files on the media. Controls might include encryption of the media with keys assigned to given users, a secret key, PIN or user account managed access, etc. Verify the methods meet NRC-defined requirements.

B.11.3 MP-3 MEDIA-MARKING

Interview

How does your organization mark system media? Are procedures available explaining how the media must be marked?

Is any media exempt from marking? If so, why?

Examine

Review media protection documentation to determine whether the organization:

- Marks system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
- Exempts NRC defined types of system media from marking as long as the media remain within NRC defined controlled areas.

Review a sample of system media to ensure that the organization marks system media in accordance with NRC defined requirements.

Test

Arrange with the system team to observe a walk-through of how system personnel follow the organizational processes for marking information media; automated mechanisms supporting and/or implementing media marking and verify the processes meet all NRC-define requirements for media marking, especially for media with sensitive data.

B.11.4 MP-4 MEDIA-STORAGE

Interview

How and where does your organization store digital and non-digital media?

What physical controls are in place for the controlled storage areas?

How is system media securely stored?

Examine

Review media protection documentation to determine whether the organization:

Physically controls and securely stores NRC defined types of digital and non-digital media within NRC defined controlled areas; and

Protects system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Inspect the physical storage location and access enforcement mechanisms for digital system media to ensure that the organization restricts access to digital system media until the media is destroyed or sanitized and in accordance with NRC defined requirements.

Inspect the physical storage location and access enforcement mechanisms for non-digital system media, such as paper documents, to ensure that the organization restricts access to non-digital system media until the media is destroyed and in accordance with NRC defined requirements.

Test

Arrange with the system team for a walk-through of the organizational processes for storing information media, using sample media. Along with any manual processes also observe as the personnel employ any automated mechanisms they have to support and/or provide secure media storage/media protection and access restrictions. Observe the processes and mechanisms as they are used to verify that all NRC-defined media storage requirements and access limitation needs are met by the process.

B.11.5 MP-5 MEDIA-TRANSPORT

Interview

Who is authorized to transport system media outside of controlled areas? Have these personnel been documented as having this authority?

Are there non NRC personnel (e.g., couriers, U.S. Postal Service, commercial transport or delivery service) authorized to transport system media outside of controlled areas?

How are activities associated with transport of system media restricted to authorized personnel?

How is system media controlled and protected during transport outside of controlled areas?

Are all transport activities documented? If so, where?

Examine

Review media protection documentation to determine whether the organization:

- Protects and controls NRC defined types of system media during transport outside of controlled areas using NRC defined security safeguards;
- Maintains accountability for system media during transport outside of controlled areas;
- Documents activities associated with the transport of system media; and
- Restricts the activities associated with the transport of system media to authorized personnel.

Examine records of system media transport to verify that the organization protects, controls, and documents system media during transport outside of controlled areas as documented in media protection documentation and in accordance with NRC defined requirements.

Test

Arrange with organizational personnel with information system media transport responsibilities to demonstrate the procedures, processes, and tools used to securely transport media that may contain NRC sensitive information. Confirm that the media transport activities in-fact provide the media protections required by NRC-defined media transport security requirements.

Enhancement 4

Interview

Does your organization implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas? If so, what mechanisms are used?

Examine

Review media protection documentation to determine whether the organization implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Test

Request a walk-through of the organization's methods used to encrypt media. Verify the cryptographic mechanisms used are FIPS-140-2 validated and protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas as documented in media protection documentation and in accordance with NRC defined requirements. Inspecting a random sampling of media should find the encryption in use wherever any NRC sensitive files may be stored on the media.

B.11.6 MP-6 MEDIA-SANITIZATION

Interview

Does your organization sanitize system media before disposal, release out of organizational control, or release for reuse?

If so, how is the media sanitized? Are sanitization procedures documented?

Examine

Review media protection documentation to determine whether the organization:

- Sanitizes NRC defined system media prior to disposal, release out of organizational control, or release for reuse using NRC defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; and
- Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Examine records of media sanitization or other relevant media protection documentation to verify that the organization sanitizes system media as documented in media protection documentation and in accordance with NRC defined requirements.

Test

Work with the ISSO and/or system team to obtain a walkthrough test of their media sanitization methods and tools used to verify that the organization successfully sanitizes system media as documented in media protection documentation and in accordance with NRC defined requirements, using sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.

Enhancement 1

Interview

Does your organization verify that media has been sanitized properly? If so, who is responsible for verifying this? What is involved in verification? Are records maintained to support that media has been properly sanitized?

Examine

Examine records of media sanitization or other relevant media protection documentation to verify that the organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Test

Work with the ISSO and/or system team as needed to obtain a walk-through test of the organization's processes for media sanitization, including any automated mechanisms or tools they employ to support and/or implementing and manage media sanitization. Verify the sanitization processes and tools used are effective and include the following actions, as required per NRC policies and with consideration of the sensitivity of the media:

- Approves and reviews sanitization disposal actions
- Tracks and documents sanitization and disposal actions
- Verifies sanitization and disposal actions

Enhancement 2

Interview

Does your organization test sanitization equipment and procedures? If so, who is responsible for testing the equipment and procedures? Are test results documented? If so, where?

Examine

Review media protection documentation to determine whether the organization tests sanitization equipment and procedures at the NRC defined frequency to verify that the intended sanitization is being achieved.

Examine records of media sanitization testing or other relevant media protection documentation to verify that the organization tests sanitization equipment and procedures at the NRC defined frequency to verify that the intended sanitization is being achieved.

Test

Work with the ISSO and/or system team as needed to obtain and observe a walk-through test of their procedures and methods used for testing their media sanitization equipment and process. Verify that their tools and methods provide the intended sanitization, per NRC-defined media sanitization requirements.

Once the sanitization equipment or tools and process have been verified a sampling of previously sanitized media should be collected. Using the tools that have been verified as functional test any previously sanitized media to verify that they have in fact been properly sanitized as per NRC sanitization requirements.

Enhancement 3

Interview

Are there any circumstances under which your organization sanitizes portable storage devices before connecting the devices to the system? Are the circumstances communicated to system personnel? How are they communicated?

Examine

Review media protection documentation to determine whether the organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the NRC and/or the organizations defined circumstances in accordance with NRC defined requirements.

Test

Work with the system team and/or ISSO to obtain a walk-through test use of their nondestructive sanitization techniques for portable storage devices. Verify that the process and tools effectively sanitize the portable storage devices per NRC-defined requirements. The tools logs should be checked for no sanitization process errors.

B.11.7 MP-7 MEDIA-USE

Interview

Are any types of media prohibited for use on system components? If so, what are they?

What security safeguards are in place to prevent their use?

Examine

Review media protection documentation to determine whether the organization restricts or prohibits the use of NRC defined types of system media on the system in accordance with NRC defined requirements.

Test

Observe safeguards in place for NRC defined system media while in use to verify that the organization restricts or prohibits the use of such media in accordance with NRC defined requirements.

Work with the ISSO and/or system administrator to test the organization’s automated mechanisms employed to restrict or prohibit (deny) the use of NRC and/or organizationally prohibited information system media on information systems or system components. Define an authorized test scenario where prohibited media types (such as personal media) can be used in testing to verify that the automated mechanisms do detect and prevent use of organizationally defined prohibited media types.

Enhancement 1

Interview

How does your organization prevent the use of portable storage devices with no identifiable owner?

Examine

Review media protection documentation to determine whether the organization prohibits the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Test

Work with the ISSO and/or system team to arrange a live test run of any automated mechanisms the system uses to prohibit use of portable storage devices on NRC information systems or system components that have no identifiable NRC owner. Arrange for test use of an unidentified (i.e., new or unlabeled) portable storage device for this test pass, connecting the portable storage device(s) to the system in an approved location. Verify that the automated security mechanisms detect and prevent the use of the device(s).

B.12 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

Physical and environmental protection assessment objects include, but are not limited to: policy and procedures; actual physical and environmental protection mechanisms; physical access records; system component delivery and removal records; and tasks performed by organization staff in support of media protection functions.

B.12.1 PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Interview

Are system-specific physical and environmental protection procedures available?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that these reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated physical and environmental protection controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific physical and environmental protection policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.12.2 PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Systems Hosted in Non NRC Facilities:

Interview

Does your organization maintain a list of individuals with authorized access to the facility where your system resides?

Who is responsible for approving and removing access?

Who is responsible for maintaining the list of authorized individuals?

Who issues authorization credentials for access to your facility?

How often is the list of authorized individuals reviewed? Are there records to support that the reviews took place?

What is your process for requesting or removing physical access for organization staff? Is this process documented? If so, where?

Examine

Review physical and environmental protection documentation to determine whether the organization:

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

Review the access authorization list of individuals with authorized access to the facility and controlled area where the system resides to ensure the list is reviewed and updated in accordance with NRC defined requirements and that all individuals on the list require access.

Test

Work with the ISSO and physical site security office if possible to obtain a walk-through of the organization’s processes for handling physical access authorizations, including any automated tools or mechanisms they use to support and/or implement the appropriate physical access authorizations. Verify the processes effectively comply with NRC requirements for managing and providing correct physical site access authorizations.

B.12.3 PE-3 PHYSICAL ACCESS CONTROL

Systems Hosted in Non NRC Facilities:

Interview

How are all physical entry and exit points to the facility controlled?

How are individual access authorizations verified before being granted access to the facility?

Are security safeguards in place in the areas that are officially designated as publicly accessible? Please describe the safeguards.

Are physical access audit logs maintained at each entry and exit point?

Are all visitors escorted and monitored?

Who is responsible for ensuring that the physical access devices used at the facility are functioning properly? What is involved in ensuring that the device is functioning properly? Are there documented procedures for doing so?

Who is responsible for the maintenance of the devices? How often does maintenance occur?

How are facility keys, combinations and other access devices secured?

How often are keys and combinations to locks within the facility changed?

What happens when keys are lost, combinations are compromised, or individuals are transferred or terminated?

Does your organization conduct and maintain an inventory of all physical access devices? If so, how often is the inventory reviewed and updated? Are there records to demonstrate that the inventory was reviewed?

Examine

Review physical and environmental protection documentation to determine whether the organization enforces physical access authorizations in accordance with NRC defined requirements.

Review physical access audit logs to ensure that the organization tracks physical access to NRC defined entry and exit points. These logs must specify, at a minimum, the name of the individual accessing the facility and the date and time of access.

Review records that provide evidence that the organization inventories physical access devices in accordance with NRC defined requirements. These records must specify, at a minimum, what physical devices were inventoried, the date that the inventory took place, and the individual(s) who performed the inventory.

Test

Work with the ISSO and physical site security office if possible to obtain a walk-through demo of the physical access control mechanisms used at NRC defined entry and exit points to confirm that individual access authorizations are verified prior to access to the facility being granted and physical access to the facility is enforced in accordance with NRC defined requirements.

- Inspect and/or observe safeguards used to control access to areas within the facility officially designated as publicly accessible to ensure the organization controls access to such areas in accordance with NRC defined requirements.
- Observe system personnel escorting visitors to the facility (this can include the assessor(s)) to ensure that the organization escorts visitors and monitors visitor activity at all times.
- Inspect the physical storage location of keys, combinations, and other physical access devices used by or for the NRC to verify that the organization secures such physical access devices.

Enhancement 1

Interview

Does your organization enforce physical access authorization to your system in addition to the physical access controls for the hosting facility? How is physical access to the areas hosting the system (within the facility) controlled?

Examine

Review physical and environmental protection documentation to determine whether the organization enforces physical access authorizations to the system in addition to the physical access controls for the facility in accordance with NRC defined requirements.

Examine physical access logs to verify that the organization documents access to and from the NRC defined areas where the system resides.

Test

Work with the ISSO and physical site security team if possible to obtain a walk-through demo of the physical access authorization and observe to confirm that physical access control mechanisms at NRC defined physical spaces containing one or more components of the system to ensure that individual access authorizations are verified prior to access to the space being granted and physical access to the space is enforced in accordance with NRC defined requirements.

B.12.4 PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Systems Hosted in Non NRC Facilities:

Interview

How is physical access to system distribution and transmission lines within organizational facilities controlled?

Examine

Review physical and environmental protection documentation to determine whether the organization controls physical access to system distribution and transmission lines within organizational facilities using NRC defined security safeguards.

Test

Work with the ISSO and physical site security team if possible to obtain a walk-through of and observe the physical access control mechanisms in-place at NRC defined system distribution and transmission lines to verify that access protections covering NRC related transmission mediums is enforced in accordance with NRC defined requirements.

B.12.5 PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Systems Hosted in Non NRC Facilities:

Interview

How does your organization control physical access to output devices (e.g., monitors, printers, and audio devices) located within your office space?

Examine

Review physical and environmental protection documentation to determine whether the organization controls physical access to system output devices (e.g., monitors, printers, etc.) to prevent unauthorized individuals from obtaining the output.

Test

Work with the ISSO and/or office site security office where possible to obtain a walk-through of and to observe physical access control mechanisms protecting system output devices (e.g., monitors, printers, and audio devices) to confirm that the organization prevents unauthorized individuals from obtaining system output as per NRC-defined requirements

B.12.6 PE-6 MONITORING PHYSICAL ACCESS

Systems Hosted in Non NRC Facilities:

Interview

How does your organization monitor physical access to the facility and to the system?

Who is responsible for monitoring physical access to the system?

Does your organization review physical access logs? If so, how often? Who is responsible for reviewing the logs? Are there records demonstrating that the reviews took place?

Who is responsible for coordinating the results of physical access log reviews and investigations with your organization’s incident response team/capability?

Examine

Review physical and environmental protection documentation to determine whether the organization:

- Monitors physical access to the facility where the system resides to detect and respond to physical security incidents;
- Reviews physical access logs in accordance with the NRC defined frequency and upon occurrence of NRC defined events or potential indications of events; and
- Coordinates results of reviews and investigations with the organizational incident response capability.

Review records of physical access log reviews to ensure that the organization reviews such logs in accordance with NRC defined requirements.

Review records that document the details of prior system security incidents involving physical security that have occurred on the system to ensure that the organization coordinates results of reviews and investigations with the organizational incident response capability.

Test

Work with the ISSO and physical site security team if possible to obtain a walk-through of and observe the mechanisms and processes used by the organization to monitor physical access to the facility where the NRC system resides to detect and respond to physical security incidents, as per applicable NRC requirements, plans, and policies.

Enhancement 1

Systems Hosted in Non NRC Facilities:

Interview

Who is responsible for monitoring real time intrusion alarms and surveillance equipment?

Examine

Review physical and environmental protection documentation to determine whether system personnel monitor physical intrusion alarms and surveillance equipment in accordance with NRC defined requirements.

Test

Work with the ISSO and physical site security team if possible to obtain a walk-through of and observe system personnel with physical access monitoring responsibilities to verify that system personnel monitor physical intrusion alarms and surveillance equipment in accordance with NRC defined requirements. Request information on examples of how such alarms or surveillance responses were handled in recent past.

Enhancement 4

Systems Hosted in Non NRC Facilities:

Interview

How does your organization monitor physical access to the facility and to all system components within your office space?

Examine

Review physical and environmental protection documentation to determine whether the organization monitors physical access to the system in addition to the physical access monitoring of the facility in accordance with NRC defined requirements.

Test

Work with the ISSO and external or 3rd party site physical security office or team if possible to obtain a site walk-through and observe to verify how system personnel with physical access monitoring responsibilities do monitor physical access to the system in accordance with NRC defined and contractual requirements.

B.12.7 PE-8 VISITOR ACCESS RECORDS

Systems Hosted in the NRC Data Center:

Interview

Does your organization have a signed service level agreement with OIS stating that OIS will maintain and review visitor access records for the Data Center? If so, please provide the agreement.

Examine

Examine the service level agreement with OIS to ensure that the service level agreement is current and specifies that the NRC maintains and reviews visitor access logs for the system.

Test

Work with the ISSO and site physical security office as necessary to obtain a site walk-through and observe organizational processes for maintaining and reviewing visitor access records, including the use of automated mechanisms supporting and/or implementing maintenance and review of visitor access records to confirm that these security tasks are carried out in accordance with NRC policies and contractual agreements.

Systems Hosted in Non NRC Facilities:

Interview

Does your organization maintain visitor access records to the facility where your system resides? If so, how long are records retained? Who is responsible for maintaining them?

How often does your organization review visitor access records? Who is responsible for reviewing them? Are there records demonstrating that the reviews took place?

Examine

Review a sample of visitor access records to the facility where the system resides to ensure that the organization tracks visitor access to the facility and maintains and reviews visitor access records in accordance with NRC defined requirements. These records must specify, at a minimum, the name and organization of the visitor, the name of the individual responsible for escorting and supervising the visitor during the visit, the purpose of the visit, the date and time of the visitor’s arrival, and the date and time of the visitor’s departure.

Test

Work with the ISSO and external or 3rd party site physical security office or team if possible to obtain a site walk-through and observe organizational processes for maintaining and reviewing visitor access records and their content, including the use of automated mechanisms supporting and/or implementing maintenance and review of visitor access records to confirm that these security tasks are carried out in accordance with NRC policies and contractual agreements.

Enhancement 1

Systems Hosted in the NRC Data Center:

Interview

Does your organization have a signed service level agreement with OIS stating that OIS will maintain and review visitor access records for the Data Center using an automated mechanism? If so, please provide the agreement.

Examine

Examine the service level agreement with OIS to ensure that the service level agreement is current and specifies that the NRC employs automated mechanisms to facilitate the maintenance and review of visitor access records.

Test

Work with the ISSO and site physical security office or team as necessary to obtain a site walk-through and observe organizational processes for maintaining and reviewing visitor access records, including the use of automated mechanisms supporting and/or implementing maintenance and review of visitor access records to confirm that these security tasks are carried out in accordance with NRC policies and contractual agreements.

Systems Hosted in Non NRC Facilities:

Interview

Does your organization use automated mechanisms to maintain and review visitor access records? If so, what mechanisms are used, and what do they do? Who is responsible for supporting the mechanism?

Examine

Review physical and environmental protection documentation to determine whether the organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

Test

Work with the ISSO and external or 3rd party site physical security office or team if possible to obtain a site walk-through and observe organizational processes for maintaining and reviewing visitor access records and their content, including the use of automated mechanisms supporting and/or facilitating maintenance and review of visitor access records to confirm that these security tasks are carried out in accordance with NRC policies and contractual agreements.

B.12.8 PE-9 POWER EQUIPMENT AND CABLING

Systems Hosted in Non NRC Facilities:

Interview

How does your organization protect internal and external power equipment and power cabling for the system from damage and destruction?

Examine

Review physical and environmental protection documentation to determine whether the organization protects power equipment and power cabling for the system from damage and destruction.

Test

Work with the ISSO and site physical security office or team if possible to obtain a site walk-through and observe the mechanisms used to protect the power equipment and power cabling for the system to verify that the organization protects such equipment from damage and destruction. Ensure that power equipment and cabling is protected from unauthorized access as well as from environmental hazards, such as water damage, etc. as required by NRC policies and contractual requirements.

B.12.9 PE-10 EMERGENCY SHUTOFF

Systems Hosted in Non NRC Facilities:

Interview

Does your organization provide the capability to shut off power to the system or individual system components in emergency situations? If so, how?

Does your organization use emergency shutoff switches or devices to facilitate safe and easy access for personnel? If so, where are they placed?

Does your organization protect emergency power shutoff capability from unauthorized activation? If so, how?

Examine

Review physical and environmental protection documentation to determine whether the organization:

- Provides the capability of shutting off power to the system or individual system components in emergency situations;

- Places emergency shutoff switches or devices in NRC defined locations to facilitate safe and easy access for personnel; and
- Protects emergency power shutoff capability from unauthorized activation.

Test

Work with the ISSO and site physical security office or team as possible to obtain a site walk-through and observe the emergency power shutoff capability provided for the system to ensure that power shutoff switches or devices are easily and safely accessible to system personnel and are protected from unauthorized activation, and complies with NRC-defined contractual requirements and security policies.

B.12.10 PE-11 EMERGENCY POWER

Systems Hosted in the NRC Data Center:

Interview

Does your organization have a signed service level agreement with OIS stating that OIS will ensure that your system is connected to an NRC provided uninterruptible power supply? If so, please provide the agreement.

Examine

Examine the service level agreement with OIS to ensure that the service level agreement is current and specifies that the NRC provides a short term uninterruptible power supply for the system.

Test

Work with the ISSO and site operations staff or system administrator team as possible to obtain a site walk-through and inspect any automated mechanisms supporting and/or implementing an uninterruptible power supply for the system, and/or the supply itself. Verify that the Uninterruptible Power Supply (UPS) resource provided meets NRC-defined requirements for the system and this control.

Systems Hosted in Non NRC Facilities:

Interview

Does your organization provide a short term uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a loss of the primary power source?

Examine

Review physical and environmental protection documentation to determine whether the organization provides a short term uninterruptible power supply to facilitate an orderly shutdown of the system or the transition of the system to long term alternate power in the event of a primary power source loss in accordance with NRC defined requirements.

Test

Work with the ISSO and site operations staff or system administrator team as possible to obtain a site walk-through and inspect the short term uninterruptible power supply for the system to verify that:

- The system is capable of facilitating an orderly shutdown of the system in the event of a loss of the primary power source.
- The uninterruptible power supply has sufficient battery life to provide sufficient power to the system in the event of an emergency.

Enhancement 1

Systems Hosted in Non NRC Facilities:

Interview

Does your organization provide a long term alternate power supply that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source?

Examine

Review relevant system documentation to determine whether the system is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Test

Work with the ISSO and 3rd party site operations staff or system administrator team as possible to obtain a site walk-through and inspect the long term alternate power supply to ensure that the system is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

B.12.11 PE-12 EMERGENCY LIGHTING

Systems Hosted in Non NRC Facilities:

Interview

Does your organization provide automatic emergency lighting for the system that activates in the event of a power outage or disruption? Are all emergency exits and evacuation routes within the facility covered?

Examine

Review physical and environmental protection documentation to determine whether the organization employs and maintains automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Test

Work with the ISSO and 3rd party site operations staff or system administrator team as possible to obtain a site walk-through and inspect the automatic emergency lighting capability for the system to confirm that it can and does activate in the event of a power outage or disruption and that all emergency exits and evacuation routes within the facility are covered.

B.12.12 PE-13 FIRE PROTECTION

Systems Hosted in Non NRC Facilities:

Interview

Does your organization provide fire suppression and detection devices/systems for your system that are supported by an independent energy source?

Examine

Review physical and environmental protection documentation to determine whether the organization employs and maintains fire suppression and detection devices/systems for the system that are supported by an independent energy source.

Test

Work with the ISSO and site operations staff or system administrator team as possible to obtain a site walk-through and inspect fire suppression and detection devices/systems for the system to ensure that they are supported by an independent energy source, as per NRC policies and contractually agreed requirements.

Work with the ISSO and site operations staff or system administrator team as possible to obtain a site walk-through and inspect fire suppression and detection devices/systems for the system to ensure that components of the system are not in danger of being damaged in the event a fire suppression mechanism is activated, for instance water sprinklers potentially causing damage to servers or other electronic system components, as per NRC policies and contractually agreed requirements.

Enhancement 1

Systems Hosted in Non NRC Facilities:

Interview

Does the fire detection device/system automatically notify organization personnel and emergency responders in the event of activation?

Examine

Review physical and environmental protection documentation to determine whether fire suppression and detection devices/systems deploy automatically and notify NRC defined personnel and emergency responders in the event of a fire.

Test

Contact the ISSO and/or site operations staff as appropriate to request officially valid evidence of their fire-suppression system testing. Fire departments and other officials or vendors should have inspected and/or tested the fire suppression systems. Confirm that the evidence verifies the fire suppression and detection devices/systems for the system can deploy automatically and notify emergency responders as well as site and NRC defined personnel in the event of a fire, and as per contractual agreements.

Enhancement 2

Systems Hosted in Non NRC Facilities:

Interview

Does the fire suppression device/system automatically notify organization personnel and emergency responders in the event of activation?

Examine

Review physical and environmental protection documentation to determine whether fire suppression and detection devices/systems automatically notify NRC defined personnel and emergency responders if they are activated, as per NRC policies and contractually agreed requirements. Test

Contact the ISSO and/or site operations staff as appropriate to request officially valid evidence of their fire-suppression system testing. Fire departments and other officials or vendors should have inspected and/or tested the fire suppression systems. Confirm that the evidence verifies the fire suppression and detection devices/systems for the system can deploy automatically and notify emergency responders as well as site and NRC defined personnel in the event of a fire, and as per contractual agreements.

Enhancement 3

Systems Hosted in Non NRC Facilities:

Interview

Does the fire suppression device/system automatically activate in the event that the facility is not staffed?

Examine

Review physical and environmental protection documentation to determine whether fire suppression and detection devices/systems deploy automatically even if the facility is not staffed on a continuous basis.

Test

Contact the ISSO and/or 3rd party site operations staff as appropriate to request officially valid evidence that their fire suppression and detection devices/systems for the system have been adequately tested to verify that they will deploy automatically even if the facility is not staffed on a continuous basis.

B.12.13 PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Systems Hosted in Non NRC Facilities:

Interview

How are regular levels of temperature and humidity within the facility where the system resides maintained?

How is the temperature and humidity monitored?

Examine

Review physical and environmental protection documentation to determine whether the organization:

- Maintains temperature and humidity levels within the facility where the system resides at NRC defined acceptable levels; and
- Monitors temperature and humidity levels in accordance with the NRC defined frequency.

Examine records that indicate that the organization monitors temperature and humidity levels in accordance with the NRC defined frequency.

Test

Contact the ISSO and/or site operations staff as appropriate to request officially valid evidence that their mechanisms used to monitor temperature and humidity levels within the facility and areas where the system resides successfully monitor temperature and humidity levels in the facility and ensures the levels are kept within NRC defined acceptable levels, and per contractual agreements with the NRC.

B.12.14 PE-15 WATER DAMAGE PROTECTION

Systems Hosted in Non NRC Facilities:

Interview

Which key personnel know where to locate and activate the master shutoff valves for plumbing system? Are operational procedures available? If so, where?

How is the system protected from water damage resulting from broken plumbing lines or other sources of water leakage?

How does your organization ensure that the master shutoff valves are accessible, working properly, and known to key personnel?

Examine

Review physical and environmental protection documentation to determine whether the organization protects the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Test

Work with the ISSO and site operations staff or system administrator team as possible to obtain a site walk-through and inspect master water shutoff or isolation valves to ensure that the organization is able to protect the system from damage resulting from water leakage and that the valves are accessible, working properly, and known to key personnel.

Inspect any other water damage protection mechanisms that may be in place, such as floor drains intended to ensure adequate water protections for the system, as per NRC-defined requirements for this control and contractual agreements.

Enhancement 1

Systems Hosted in Non NRC Facilities:

Interview

Does your organization use automated mechanisms to detect the presence of water in close proximity to the system? If so, does the mechanism automatically alert responsible personnel?

Examine

Review physical and environmental protection documentation to determine whether automated mechanisms are used to detect the presence of water in close proximity to the system and whether the mechanisms automatically alert NRC defined personnel.

Test

Work with the ISSO and site operations staff as possible to obtain a site walk-through and inspect the automated mechanisms used to detect the presence of water in close proximity to the system to ensure that the mechanism is able and configured to automatically alert the proper site and NRC defined personnel.

B.12.15 PE-16 DELIVERY AND REMOVAL

Interview

Who is responsible for authorizing, monitoring, and controlling the delivery and removal of system components?

Who is responsible for Are there records demonstrating that the delivery and removal was approved, monitored, and controlled?

Are delivery areas controlled?

Are delivery areas isolated from the system and media libraries?

Examine

Review records of NRC defined system components entering and exiting the facility to ensure that the organization authorizes, monitors, and controls the delivery and removal of system components. These records must specify, at a minimum, the date and time the system component was delivered or removed and the individual(s) who received the delivery or oversaw the removal.

Test

Work with the ISSO and site operations staff as possible to obtain a site walk-through to observe authorized personnel demonstrate their processes for receiving deliveries and removing system components as per NRC-defined security requirements.

Inspect delivery areas to confirm that such areas are isolated from the system and media libraries, not affording unauthorized personnel access to NRC systems or data.

B.12.16 PE-17 ALTERNATE WORK SITE

Interview

Does your organization maintain an alternate work site (or work sites)?

If so, is the effectiveness of security controls assessed at the work sites?

How do employees located at alternate work sites communicate with information security personnel if a security incident or problem occurs?

Examine

Review physical and environmental protection documentation to determine whether the organization:

- Employs NRC defined security controls at alternate work sites;
- Assesses as feasible, the effectiveness of security controls at alternate work sites; and
- Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Examine records of security control assessments conducted at the alternate work site to verify that the organization employs and assesses security controls at the alternate work site in accordance with NRC defined requirements.

Test

Work with the ISSO and a sampling of system team personnel that are able to work remotely to obtain a walk-through demo of how they handle user or system security when working at alternate sites (i.e., home) as authorized by the NRC, and per the applicable NRC policies and processes. Confirm their observed use of NRC-approved processes and tools for security at alternate work sites, including any automated mechanisms supporting their work at alternate sites meets NRC-defined requirements.

B.12.17 PE-18 LOCATION OF SYSTEM COMPONENTS

Interview

When positioning system components within your facility, what issues did you consider?

How does the location of the components address the issues?

Examine

Review physical and environmental protection documentation to determine whether the organization positions system components within the facility to minimize potential damage from NRC defined physical and environmental hazards and to minimize the opportunity for unauthorized access.

Test

Work with the ISSO and site operations staff as possible to obtain a site walk-through of the systems components as located in their operating site(s). Inspect the location of system components as installed to ensure that they are positioned in a manner that minimizes the potential damage from NRC defined physical and environmental hazards and minimizes the opportunity for unauthorized access.

B.13 SECURITY PLANNING (PL)

Security planning assessment objects include, but are not limited to: policy and procedures; system-specific rules of behavior; information security architecture documents; and tasks performed by organization staff in support of planning functions.

B.13.1 PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Interview

Are system-specific security planning procedures available?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated security planning controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific security planning policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.13.2 PL-2 SYSTEM SECURITY PLAN

<u>Interview</u>

Has a security plan consistent with NIST SP 800-18 been developed for the system?

Has the security plan been implemented?

Who is responsible for reviewing, updating, and approving the security plan?

How often is the plan reviewed and updated?

Who is responsible for:

- Defining the system's authorization boundary?
- Describing how the system supports the organization's missions and business processes?
- Describing the operational environment and relationships with or connections to other systems?
- Describing the implementation of specific security controls?
- Explaining the plan for implementing security controls that are not currently implemented.

Are there records to support that reviews and updates to the plan took place?

Who is responsible for distributing the plan to organization personnel? Are there records to support that the plan was distributed?

<u>Examine</u>

Review the SSP to determine whether the SSP:

- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the system in terms of missions and business processes;
- Provides the security categorization of the system including supporting rationale;
- Describes the operational environment for the system and relationships with or connections to other systems;
- Provides an overview of the security requirements for the system;
- Identifies any relevant overlays, if applicable;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

Evaluate the implementation details for each security control for accuracy and completeness per CSO-PROC-2104, "System Artifact Examination Procedure."

Evaluate the rationale for security controls that have been tailored out of the system's security control baseline:

- To determine whether the risk associated with removing the security control from the baseline is consistent with the agency's current risk tolerance level.
- For accuracy and completeness per CSO-PROC-2104, "System Artifact Examination Procedure."

Review the revision history in the SSP to verify that the organization reviews and updates the SSP in accordance with NRC defined requirements.

Enhancement 3

Interview

When developing the plan, did your organization consult other organizations that might be impacted by security related activities that might impact them when the activities are conducted?

Examine

Review the SSP to determine whether the organization plans and coordinates security related activities affecting the system with NRC defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.

B.13.3 PL-4 RULES OF BEHAVIOR

Interview

Does your organization have a documented set of rules concerning user responsibilities and expected behavior with regard to use of the system? If so, where is the document?

Are these rules available to all system users?

How are the rules disseminated to the users?

Are users required to re-sign an acknowledgement that indicates that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the system and its resident information?

Where are the acknowledgements archived?

Are users informed and required to resign the acknowledgement when the rules of behavior are updated or revised?

Examine

Review system-specific rules of behavior to determine whether the organization:

- Establishes and makes readily available to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior with regard to information and system usage.
- Reviews and updates the rules of behavior in accordance with the NRC defined frequency.

Examine a sample of signed acknowledgements from users indicating that they have read, understand, and agree to abide by the rules of behavior to verify that the organization:

- Requires such acknowledgement before authorizing access to the system; and
- Requires 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.

Test

Arrange a walk-through with the system team as necessary to obtain a walk-through of the organizational processes for establishing, reviewing, disseminating, and updating rules of behavior, including their use of any automated mechanisms supporting and/or implementing the establishment, review, dissemination, and update of rules of behavior.

Verify that the process can effectively distribute, obtain user signatures on, and manage the rules of behavior as per NRC-defined requirements.

Enhancement 1

Interview

Are explicit restrictions concerning the use of social media and networking sites included in the rules of behavior?

Are explicit restrictions concerning posting organizational information on public websites included in the rules of behavior?

Examine

Review system-specific rules of behavior to determine whether the organization includes explicit restrictions on the use of social media/networking sites and posting organizational information on public websites in the rules of behavior.

Test

Arrange a walk-through with the system team as necessary to obtain a walk-through of the organizational processes for establishing, reviewing, disseminating, and updating rules of behavior, including their use of any automated mechanisms supporting and/or implementing the establishment, review, dissemination, and update of rules of behavior. Verify that the process can effectively distribute and manage the rules.

B.13.4 PL-8 INFORMATION SECURITY ARCHITECTURE

Interview

Does your organization have documented information security architecture for your system that explains your approach to protecting the confidentiality, integrity, and availability of organizational information?

If so, where is the architecture documented?

Who is responsible for documenting the architecture?

Does your organization coordinate the development and maintenance of the system’s information security architecture with organizations responsible for the enterprise architecture?

Are changes to the information security architecture reflected in the system’s security plan, security Concept of Operations (CONOPS), and organizational procurements and acquisitions? Are records available to indicate that the changes were incorporated?

Examine

Review the system security architecture document or other relevant system documentation to determine whether the information security architecture for the system:

- Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
- Describes how the information security architecture is integrated into and supports the enterprise architecture; and
- Describes any information security assumptions about, and dependencies on, external services.

Review the system security architecture document or other relevant system documentation to determine whether the organization reviews and updates the information security architecture in accordance with the NRC defined frequency to reflect updates in the enterprise architecture.

Review the system security architecture document or other relevant system documentation to determine whether the information security architecture for the system is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

Review the SSP and other relevant system documentation to verify that the organization ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

B.14 PERSONNEL SECURITY (PS)

Personnel security assessment objects include, but are not limited to: personnel termination records; personnel transfer records; system access agreements; third party provider contracts; and tasks performed by organization staff in support of personnel security functions.

B.14.1 PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Interview

Are personnel security procedures available?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated personnel security controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific personnel security policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.14.2 PS-2 POSITION RISK DESIGNATION

Interview

Has a risk designation been assigned to all organizational positions? Where is the risk designation documented? Where are the risk designations defined?

Who is responsible for reviewing, updating, and approving the risk designations?

Has screening criteria been established for individuals filling the positions?

How often are the risk designations reviewed and updated?

Are there records to support that reviews and updates to the plan took place?

Examine

Review the risk designation documentation to determine whether the documentation:

- Defines each designation;
- Defines position screening criteria;
- Is consistent with the organization’s positions;
- Explicitly defines the risk designation for each position; and
- Is reviewed and updated at the organization’s required frequency.

B.14.3 PS-3 PERSONNEL SCREENING

Interview

Are all individuals screened prior to being granted access to the system?

Are conditions requiring re-screening documented?

Is the frequency of re-screening documented?

Are individuals re-screened in accordance with defined conditions?

Examine

Review personnel screening documentation to determine if the documentation:

- Contains conditions for personnel re-screening;-
- Contains a record of screening individuals prior to being granted system access; and
- Contains a record of re-screening individuals in accordance with the defined conditions.

B.14.4 PS-4 PERSONNEL TERMINATION

Interview

When personnel are terminated, what takes place? Is the termination procedure documented? If so, where?

Who is responsible for ensuring that the termination procedures is followed? Are records maintained to demonstrate that required activities were performed?

Examine

Review personnel security documentation to determine whether the organization:

- Disables system access within the NRC defined time period;
- Terminates/revokes any authenticators/credentials associated with the individual;
- Conducts exit Interviews that include a discussion of NRC defined information security topics;
- Retrieves all security related organizational system related property;
- Retains access to organizational information and systems formerly controlled by terminated individual; and
- Notifies NRC defined personnel within the NRC defined time period.

Examine records of personnel termination to verify that the organization takes the appropriate actions upon termination of individual employment in accordance with NRC defined requirements.

Test

Work with the organizational supervisory staff and/or ISSO to obtain a walk-through test of and observe their processes used to process personnel termination; including any automated mechanisms used to supporting and/or communicate personnel termination notifications. Verify that any processes or automated mechanisms used for disabling information system access/revoking authenticators successfully revoke and disable any access for the terminated personnel as per NRC-defined policies.

Enhancement 2

Interview

Does your organization employ automated mechanisms to notify NRC defined personnel in the event that an individual is terminated?

Examine

Review relevant system documentation to determine whether the organization uses automated mechanisms to notify NRC defined personnel in the event that an individual is terminated.

Test

Work with the organizational supervisory staff and/or ISSO to obtain a walk-through test use of any processes and automated mechanisms the organization uses to notify NRC defined personnel in the event that an individual is terminated. To test this a simulated scenario discharging a simulated/test user may be carried out. Confirm that the processes used are effective and meet all NRC requirements for disabling and/or revoking system, data, and site access of discharged users as appropriate.

B.14.5 PS-5 PERSONNEL TRANSFER

Interview

When personnel are terminated, what takes place? Is the termination procedure documented? If so, where?

Who is responsible for ensuring that the termination procedures is followed? Are records maintained to demonstrate that required activities were performed?

Examine

Review personnel security documentation to determine whether the organization:

- Reviews and confirms ongoing operational need for current logical and physical access authorizations to systems/facilities when individuals are reassigned or transferred to other positions within the organization;
- Initiates NRC defined transfer or reassignment actions within the NRC defined time period 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 within the NRC defined time period.

Examine records of personnel transfer to verify that the organization takes the appropriate actions when individuals are reassigned or transferred to other positions within the organization in accordance with NRC defined requirements.

Test

Work with the organizational supervisory staff and/or ISSO to obtain a walk-through test of any processes and automated mechanisms that the organization uses to notify NRC defined personnel if/when an individual is transferred. A simulated scenario transferring a test user may be carried out. Confirm that the processes used are effective and meet all NRC requirements for disabling and/or revoking system, data, and site access of transferred users as appropriate.

B.14.6 PS-6 ACCESS AGREEMENTS

Interview

Does your organization require users to sign access agreements before access is granted to the system? If so, where are the agreements archived?

Who is responsible for reviewing the agreements? How often are they reviewed?

Examine

Review a sample of system access agreements to determine whether the organization:

- Develops and documents access agreements for organizational systems;
- Reviews and updates the access agreements in accordance with the NRC defined frequency.

□ Review a sample of system access agreements to determine whether the system users:

- Sign appropriate access agreements prior to being granted access; and
- Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or in accordance with the NRC defined frequency.

Test

Arrange with the system team as necessary to obtain a walk-through test of the organizational processes for establishing, reviewing, disseminating, and updating user access agreements, including their use of any automated mechanisms supporting and/or implementing the establishment, review, dissemination, and update access agreements. Verify that the process can effectively and timely distribute, collect user acceptance of, and manage the agreements per NRC-defined requirements.

B.14.7 PS-7 THIRD PARTY PERSONNEL SECURITY

Interview

Who is responsible for monitoring third party security personnel compliance with NRC requirements? How is non-compliance handled? Who is non-compliance reported to?

Examine

Review third party provider contracts or other relevant system documentation to determine whether the organization:

- 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 the organization;
- Documents personnel security requirements;
- Requires third party providers to notify NRC defined personnel of any personnel transfers or terminations of third party personnel who possess organizational credentials and/or badges, or who have system privileges within the NRC defined time period; and
- Monitors provider compliance.

Test

Arrange with the system ISSO and team to perform a walk-through test of the organizational processes for managing and monitoring third-party personnel security, including any automated mechanisms used in supporting and/or implementing the monitoring of 3rd party provider compliance. Verify the process adequately inspects and confirms the personnel security compliance of the 3rd party providers.

B.14.8 PS-8 PERSONNEL SANCTIONS

Interview

Is a formal personnel sanction process documented? Where?

Is a formal sanctions process employed for individuals failing to comply with established information security policies and procedures?

Who is notified when a formal employee sanctions process is initiated?

What is the time period within which the notification must occur?

Examine

Review personnel sanction documentation to determine whether the organization:

- Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures;
- Defines personnel or roles to be notified when a formal employee sanctions process is initiated;
- Defines the time period within which organization-defined personnel or roles must be notified when a formal employee sanctions process is initiated; and
- notifies organization-defined personnel or roles within the organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

B.15 RISK ASSESSMENT (RA)

Risk assessment objects include, but are not limited to: policy and procedures; system security categorization; security risk assessment; vulnerability assessment report; periodic scan report; and tasks performed by organization staff in support of risk assessment functions.

B.15.1 RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Interview

Does your organization have system-specific risk assessment procedures? If so, where are they archived, and who is responsible for maintaining them?

How often are the procedures disseminated, reviewed, and updated? Are there records to support that the reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated risk assessment controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific risk assessment policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.15.2 RA-2 SECURITY CATEGORIZATION

Interview

Has a security categorization of your system been conducted? When was the security categorization approved?

Who is responsible for maintaining the security categorization? Under what circumstances is the security categorization reviewed and updated? Do you have records to demonstrate that the reviews took place?

Who was involved in the categorization? Did you consult other organizations impacted by the categorization of the system?

Who was responsible for identifying each of the information types? For evaluating the impact levels?

Who was responsible for identifying each data type, and for describing the data type flow?

Who was responsible for evaluating the system for privacy information, and for explaining how the system processes, stores, transmits, and uses the information?

<u>Examine</u>

Review the system Security Categorization document to verify that the organization:

- Categorizes information and the 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 system; and
- Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Review the system Security Categorization is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

<u>Test</u>

Work with the ISSO to obtain a walk-through of procedures used by the organization to establish the appropriate security categorization of the system, and/or its data. Observe and confirm that the process adequately addresses all NRC-defined requirements for security categorization of the information system assets or data.

B.15.3 RA-3 RISK ASSESSMENT

<u>Interview</u>

Does your organization conduct risk assessments to determine the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and systems that support your operations and assets?

If so, where are the assessment results documented?

Who is responsible for conducting the risk assessments? How often are the results reviewed?

Under what circumstances is the risk assessment updated?

Are there records to demonstrate that the reviews and updates took place?

<u>Examine</u>

Review the system Security Risk Assessment to verify that the organization:

- Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system and the information it processes, stores, or transmits;
- Documents risk assessment results in accordance with NRC defined requirements;
- Reviews risk assessment results in accordance with the NRC defined frequency;
- Disseminates risk assessment results to NRC defined personnel; and
- Updates the risk assessment in accordance with the NRC defined frequency or whenever there are significant changes to the system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Review the system Security Risk Assessment to verify that the Security Risk Assessment is documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

Test

Work with the system ISSO and security team to obtain a walk-through (table-top exercise) of how the organization carries out processes for risk assessment; including their use of any automated mechanisms (such as documentation systems) supporting and/or used for conducting, documenting, reviewing, disseminating, and updating the risk assessment. Confirm that the processes used adequately address each of the following risk assessment objectives, per NRC-defined requirements:

- Conducts an assessment of risk, including the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the data it processes, stores, or transmits;
- Documents risk assessment results in the NRC-defined report types;
- Reviews risk assessment results on the NRC-defined frequency; and
- Disseminates risk assessment results to the NRC-defined personnel or roles; and updates the risk assessment on the NRC-defined frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact or change the security state of the system.

B.15.4 RA-5 VULNERABILITY SCANNING

Interview

How often does your organization conduct vulnerability scans of the system and hosted applications?

Who is responsible for performing vulnerability scans on the system?

Who is responsible for analyzing vulnerability scan reports and security control assessment results?

Who is responsible for remediating vulnerabilities?

Does your organization share information obtained from vulnerability scans and security control assessments with other organizations? If so, which organizations?

Does the system have custom code? If so, where can the custom code be found?

Examine

Review the system vulnerability assessment reports, periodic scan reports, or other relevant system documentation to verify that the organization:

- Scans for vulnerabilities in the system and hosted applications in accordance with the NRC defined frequency and/or randomly in accordance with NRC defined requirements and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- Employs NRC approved vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process.

Review the results of the most recent vulnerability scans conducted to ensure that the organization scans for vulnerabilities in accordance with NRC defined requirements.

Review the results of the most recent vulnerability scans conducted to ensure that the organization documents the results of vulnerability scans in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

Compare the results of the most recent vulnerability scans to findings in the system POA&M to ensure that the organization analyzes vulnerability scan reports and results from security control assessments and remediates legitimate vulnerabilities in accordance with NRC defined requirements.

Review the system to determine if custom code exists in the system. Identify a representative sample of the custom code.

Test

Work with the system ISSO and/or security team to obtain a walk-through test of how the organization performs processes for vulnerability scanning and assessment; including their use of any automated mechanisms automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and vulnerability report data sharing, as per NRC-defined requirements. Confirm that the processes used adequately satisfy each of the NRC-required vulnerability scanning and management objectives.

Perform a code review of the sample of custom code and identify risks associated with the custom code.

Enhancement 1

Interview

What tools are used to conduct vulnerability scans? How are they updated?

Examine

Review a sample of past system vulnerability assessment reports and/or periodic scan reports to verify that the organization employs NRC approved vulnerability scanning tools and techniques.

Test

Work with the system ISSO and/or security team to obtain a walk-through test of how the organization updates their vulnerability scanning tools. Observe the tool update process to confirm the tools are in-fact updated to include latest vulnerabilities to be scanned per NRC requirements.

Enhancement 2

Interview

How often are vulnerability scanning tools updated with the latest definitions?

Examine

Review the system vulnerability assessment reports, periodic scan reports, or other relevant system documentation to verify that the organization updates the system vulnerabilities scanned in accordance with NRC defined requirements.

Test

Work with the system ISSO and/or security team to exercise the organization's processes for updating their vulnerability scanning tools, including automated mechanisms or tools supporting and/or performing vulnerability scanning tool updates used for detecting current information system vulnerabilities on at least one or more of the following conditions:

- On the NRC-defined scanning tool update frequency;
- Prior to a new vulnerability scan;
- And/or when new vulnerabilities are identified and reported.

Enhancement 4

Interview

Does your organization proactively identify information about your system that could be discovered by adversaries? If so, how? Who is notified that discoverable information exists?

Examine

Review the system vulnerability assessment reports, periodic scan reports, or other relevant system documentation to verify that the organization determines what information about the system is discoverable by adversaries and subsequently takes NRC defined corrective actions.

Test

Arrange with the ISSO and/or system security team to test any automated mechanisms they use in supporting and/or implementing risk responses based on vulnerabilities discovered during vulnerability scans and assessments. Confirm that the processes used meet the NRC-defined requirements for this security control and vulnerability related risk management.

Enhancement 5

Interview

Does your organization identify and document system components for which privileged access authorization is required during scanning? If so, where is this documented?

Examine

Review the system vulnerability assessment reports, periodic scan reports, or other relevant system documentation to verify that the system implements privileged access authorization to NRC identified system components for selected NRC defined vulnerability scanning activities.

Test

Arrange with the ISSO and/or system security team to test any automated mechanisms they use in supporting and/or implementing vulnerability scanning and tools, and privileged access requirements to perform scans. Confirm that the processes used meet the NRC-defined requirements for privileged scanning security as per NRC-defined requirements for this control.

B.16 SYSTEM AND SERVICES ACQUISITION (SA)

System and services acquisition assessment objects include, but are not limited to: policy and procedures; organizational programming and budgeting documentation; system design documentation; external system services provider agreements; developer documentation; and tasks performed by organization staff in support of system and services acquisition functions.

B.16.1 SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Interview

Are system-specific system and services acquisition procedures available?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated system and services acquisition controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific system and services acquisition policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.16.2 SA-2 ALLOCATION OF RESOURCES

Interview

How does your organization determine the information security requirements for the system or system service during mission/business process planning?

Does your organization document and allocate the resources required to protect the system or service as part of your capital planning and investment control process? If so, where is this documented?

Has your organization established a discrete line item for information security in your organization’s programming and budgeting documentation?

Examine

Review the system’s Exhibit 300 or other relevant system documentation to verify that the organization:

- Determines information security requirements for the system or system service in mission/business process planning;
- Determines, documents, and allocates the resources required to protect the system or system service as part of its capital planning and investment control process; and
- Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Test

Work with the ISSO and system team and stakeholders as necessary to obtain a walk-through of the organization’s processes for determining information security requirements. Confirm that the security requirements development process meets all the NRC-defined requirements for this control.

B.16.3 SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Interview

Is the system managed using a system development lifecycle (SDLC) methodology?

Does the SDLC methodology include information security considerations?

Are information roles and responsibilities defined and documented throughout the SDLC? If so, are individuals with the roles and responsibilities identified?

Does your organization integrate the information security risk management process into SDLC activities?

Examine

Review system and services acquisition documentation to verify that the organization:

- Manages the system using the NRC defined system development life cycle that incorporates information security considerations;
- Defines and documents information security roles and responsibilities throughout the system development life cycle;
- Identifies individuals having information security roles and responsibilities; and
- Integrates the organizational information security risk management process into system development life cycle activities.

B.16.4 SA-4 ACQUISITION PROCESS

Interview

Are the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contracts 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;
  - ✓ The environment in which the system is intended to operate; and
  - ✓ System acceptance criteria.

Examine

Review system and services acquisition documentation to verify that the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contracts 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;
  - ✓ The environment in which the system is intended to operate; and
  - ✓ System acceptance criteria.

Enhancement 1

Interview

Is the developer of the information system, system component, or information system service required to provide a description of the functional properties of the security controls to be employed?

Examine

Examine system acquisition and COR documentation to determine if the developer of the information system, system component, or information system service has provided a description of the functional properties of the security controls to be employed.

Examine developer delivered documentation to determine if the developer has provided a description of the functional properties of the security controls to be employed.

Enhancement 2

Interview

What level of detail is the developer required to provide in design and implementation information for the security controls to be employed in the information system, system component, or information system service?

Is there a definition of the design/implementation information that the developer is to provide for the security controls to be employed?

Is the developer required to provide design and implementation information for the security controls to be employed that includes, at the organization-defined level of detail, one or more of the following:

- security-relevant external system interfaces;
- high-level design;
- low-level design;
- source code;
- hardware schematics; and
- organization-defined design/implementation information.

Examine

Examine system acquisition and development documentation to determine the level of detail is the developer required to provide in design and implementation information for the security controls to be employed in the information system, system component, or information system service;

Examine system acquisition and development documentation to determine if there is a definition of the design/implementation information that the developer is to provide for the security controls to be employed;

Examine system acquisition and development documentation to determine if the developer is required to provide design and implementation information for the security controls to be employed that includes, at the organization-defined level of detail, one or more of the following:

- security-relevant external system interfaces;
- high-level design;
- low-level design;
- source code;
- hardware schematics; and
- organization-defined design/implementation information.

Examine developer delivered documentation to determine:

- The level of detail the developer provided in design and implementation information for the security controls to be employed in the information system, system component, or information system service;
- If the developer provided a description of the security controls to be employed; and
- If the developer provided design and implementation information for the security controls to be employed that includes, at the organization-defined level of detail, one or more of the following:
  - ✓ security-relevant external system interfaces;
  - ✓ high-level design;
  - ✓ low-level design;
  - ✓ source code;
  - ✓ hardware schematics; and
  - ✓ organization-defined design/implementation information.

Enhancement 9

Interview

Is the developer of the information system, system component, or information system service required to identify the following early in the system development life cycle:

- the functions intended for organizational use;
- the ports intended for organizational use;

- the protocols intended for organizational use; and
- the services intended for organizational use.

Examine

Examine system acquisition and development documentation to determine if the developer of the information system, system component, or information system service is required to identify the following early in the system development life cycle:

- the functions intended for organizational use;
- the ports intended for organizational use;
- the protocols intended for organizational use; and
- the services intended for organizational use.

Examine developer delivered documentation to determine if the developer identified the following early in the system development life cycle:

- the functions intended for organizational use;
- the ports intended for organizational use;
- the protocols intended for organizational use; and
- the services intended for organizational use.

Enhancement 10

Interview

Does the system employ only information technology products on the FIPS-201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems?

Examine

Examine system documentation to determine if the system employs only information technology products on the FIPS-201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Examine the system to determine if the system employs only information technology products on the FIPS-201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Test

Work with the ISSO and system team and stakeholders as necessary to obtain a walk-through of the system authentication mechanisms for the Personal Identity Verification (PIV) capability. Confirm that the system employs only information technology products on the FIPS-201-approved products list for Personal Identity Verification (PIV) capability.

B.16.5 SA-5 INFORMATION SYSTEM DOCUMENTATION

Interview

Does your organization have information for configuring, installing, and operating the system, system component, or service?

Is information available that effectively describes the security features in the system, component, or service?

Are known vulnerabilities concerning the configuration and use of administrative (privileged) functions documented?

Does your organization have user documentation for the system, component, or service that addresses features, capabilities, and user responsibilities for securely using or maintaining the system, component, or service?

If your organization does not have this documentation, have you attempted to obtain it? If so, are there records to demonstrate that an attempt has been made?

How is this documentation distributed?

How is this documented protected?

Examine

Review system and services acquisition documentation to verify that the organization:

- Obtains administrator documentation for the system, system component, or system service that describes:
  - ✓ Secure configuration, installation, and operation of the system, component, or service;
  - ✓ Effective use and maintenance of security functions/mechanisms; and
  - ✓ Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
- Obtains user documentation for the system, system component, or system service that describes:
  - ✓ User accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
  - ✓ Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
  - ✓ User responsibilities in maintaining the security of the system, component, or service;

Examine records that indicate that the organization documents attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent;

Inspect system documentation storage and access control mechanisms to verify that the organization:

- Protects documentation as required, in accordance with the risk management strategy; and
- Distributes documentation to NRC defined personnel.

Observe access enforcement mechanisms for system documentation to ensure that the organization protects documentation in accordance with the NRC risk management strategy.

Test

Work with the ISSO and system team as necessary to obtain a walk-through of the organizational processes used for obtaining, protecting, and distributing information system administrator and user documentation. Confirm that NRC-defined security requirements for this control (such as access to or updating documentation) are met.

B.16.6 SA-8 SECURITY ENGINEERING PRINCIPLES

Interview

Were security engineering principles considered in the design, development, and implementation of the system?

How was this accomplished?

What security engineering principles were considered? Did the system follow the principles described in NIST SP 800-27? Is there documentation that describes the security engineering principles that were considered and how they were implemented within the system?

Has the system undergone any major upgrades or modifications? Were security engineering principles considered during the upgrades? Is there documentation that describes the security engineering principles that were considered and how they were implemented within the system?

Examine

Review system design documentation or other relevant system and services acquisition documentation to verify that the organization applies system security engineering principles in the specification, design, development, implementation, and modification of the system.

Test

Work with the ISSO and system team as necessary to obtain a walk-through of any organizational processes they use for applying security engineering principles in information system-specification, design, development, implementation, and modification. Confirm that the processes include adequate steps to incorporate and address adequate security engineering in the system, per the requirements of this control, and any NRC-defined requirements.

B.16.7 SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Interview

Does your organization require that providers of external system services comply with NRC information security requirements and employ NRC required security controls?

Does your organization define and document government oversight and user roles and responsibility with regard to the external services?

If so, are the above documented in agreements with the providers? Where are the agreements archived?

Does your organization monitor security control compliance by external providers on an ongoing basis? If so, what methods are used to monitor compliance? Are compliance results documented? If so, where?

Examine

Review external system services provider agreements or other relevant system and services acquisition documentation to verify that the organization:

- Requires that providers of external system services comply with organizational information security requirements and employ NRC defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Defines and documents government oversight and user roles and responsibilities with regard to external system services; and
- Employs NRC defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

Test

Work with the ISSO and system team as necessary to obtain a walk-through and/or demonstration of organizational processes, including any automated mechanisms, used to monitor security control compliance by external service providers on an ongoing basis. Verify that the processes and tools used satisfy the security requirements of this control, assuring the external providers employ adequate security.

Enhancement 2

Interview

Does your organization require external providers to identify the functions, ports, protocols, and other services required for the use of the external services? If so, are these documented? Where?

Examine

Review external system services provider agreements or other relevant system and services acquisition documentation to verify that the organization requires providers of NRC defined external system services to identify the functions, ports, protocols, and other services required for the use of such services.

Test

Work with the ISSO and system team as necessary to obtain a walk-through and/or demonstration of organizational processes, including any automated mechanisms, used to identify the functions, ports, protocols, and other services required for the use of the external services. Verify that the processes and tools used satisfy the security requirements of this control identifying, documenting, and handling the correct external provider ports and services requirements.

B.16.8 SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Interview

Does your organization require developers to maintain a configuration management plan to control changes to the system during development, to require authorization of changes, and to provide documentation of the plan and its implementation?

If so, does the plan document the potential security impacts of changes?

Are security flaws and flaw resolution within the system, component, or service tracked? If so, how are they tracked and who are they reported to?

Examine

Review system and services acquisition documentation to verify that the organization requires the developer of the system, system component, or system service to:

- Perform configuration management in accordance with NRC defined requirements;
- Document, manage, and control the integrity of changes to NRC defined configuration items under configuration management;
- Implement only organization approved changes to the system, component, or service;
- Document approved changes to the system, component, or service and the potential security impacts of such changes; and
- Track security flaws and flaw resolution within the system, component, or service and report findings to NRC defined personnel.

Test

Work with the ISSO and system team as necessary to obtain a walk-through and/or demonstration of organizational processes, including any automated mechanisms, used to monitor 3rd party or external provider compliance with NRC change management requirements on an ongoing basis. Observe the processes and tools used and confirm they satisfy the security requirements of this control, assuring the external providers employ adequate NRC security process requirements in their change management.

B.16.9 SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

Interview

Does your organization require the developer of the system, system component, or system service to:

- Create and implement a security assessment plan?
- Conduct security testing per NRC requirements?
- Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation?
- Implement a verifiable flaw remediation process; and
- Correct flaws identified during security testing/evaluation?

If so, are the plan, test results, and flaw remediation results documented? Where are the requirements to do the above documented?

Examine

Review system and services acquisition documentation to verify that the organization requires the developer of the system, system component, or system service to:

- Create and implement a security assessment plan;
- Perform testing/evaluation in accordance with NRC defined requirements;
- Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- Implement a verifiable flaw remediation process; and
- Correct flaws identified during security testing/evaluation.

Test

Work with the ISSO and system team as necessary to obtain a walk-through or demonstration of organizational processes, including automated mechanisms, used to monitor external provider compliance with NRC developer security testing requirements. Observe the processes and tools used and confirm they satisfy the security requirements of this control, assuring that the external providers employ adequate NRC developer security testing in their system/software development processes.

B.16.10 SA-12 SUPPLY CHAIN PROTECTION

Interview

How does your organization protect against supply chain threats to the system, system component, or system service?

Examine

Review system and services acquisition documentation to verify that the organization protects against supply chain threats to the system, system component, or system service by employing NRC defined security safeguards as part of a comprehensive, defense in breadth information security strategy.

Examine system acquisition records to verify that the organization protects against supply chain threats as documented in system and services acquisition documentation and in accordance with NRC defined requirements.

Test

Work with the ISSO and system team as necessary to obtain a walk-through or demonstration of organizational processes used to define the safeguards used for protecting against supply chain threats, including any automated mechanisms supporting and/or implementing safeguards to protect against supply chain threats. Observe the processes and tools used and confirm the security requirements of this control are satisfied, assuring that adequate NRC supply chain security safeguards are employed.

B.16.11 SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Interview

Does your organization require the developer of the system, system component, or system service to follow a documented development process? If so, where is the process documented?

Does your organization review the development process, standards, tools, and tool options/configurations [to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy NRC required security requirements? If so, how often are they reviewed? Are there records to demonstrate that the reviews took place?

Examine

Review system and services acquisition documentation to verify that the organization:

- Requires the developer of the system, system component, or system service to follow a documented development process that:
  - ✓ Explicitly addresses security requirements;
  - ✓ Identifies the standards and tools used in the development process;
  - ✓ Documents the specific tool options and tool configurations used in the development process; and
  - ✓ Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
- Reviews the development process, standards, tools, and tool options/configurations in accordance with the NRC defined frequency to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy NRC defined security requirements.

B.16.12 SA-16 DEVELOPER PROVIDED TRAINING

Interview

Does your organization require the developer to provide training on the correct use of the implemented security functions, controls, and/or mechanisms? If so, how often does training take place? Are records available to demonstrate that the training took place?

Examine

Review system and services acquisition documentation to verify that the organization requires the developer of the system, system component, or system service to provide NRC defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Examine records that indicate that developer training was provided as documented in system and services acquisition documentation and in accordance with NRC defined requirements.

B.16.13 SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Interview

Does your organization require the developer to produce a design specification and security architecture? If so, are the design specification and security architecture available for review?

Examine

Review system design specifications or other relevant system and services acquisition documentation to verify that the organization requires the developer of the system, system component, or system service to produce a design specification and security architecture that:

- Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;
- Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

B.17 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

System and communications protection assessment objects include, but are not limited to: policy and procedures; system and communications protection mechanisms and configurations; and tasks performed by organization staff in support of system and communications protection functions.

B.17.1 SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Interview

Are system-specific system and communications protection procedures available?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.

o Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated system and communication protection controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020, “Organization-Defined Values for System Security and Privacy Controls”.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific system and communications protection policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.17.2 SC-2 APPLICATION PARTITIONING

Interview

How does the system separate user functionality (including user interface services) from system management functionality?

Does the system physically or logically separate user interface services from information storage and management services?

Examine

Review relevant system documentation to determine whether user functionality (including user interface services) is physically and/or logically separated from system management functionality.

Test

Observe the design of the system and functionality of system components as implemented, as well as access enforcement mechanisms, to ensure that user functionality (including user interface services) is physically and/or logically separated from system management functionality.

Work with the ISSO and system team as necessary to obtain a walk-through test of each system interface and user console, command line, or client, accessing those interfaces in real time. Identify and understand the various user roles that may be used to login to that system. Use a sample of each account type to login to and inspect the functionality of each interface. Verify for each interface that adequate separation of user functionality from system management functionality is in place. Also privileged system administrators should not be able to run or execute their system management or administrative commands while logged in with any of the systems end-user or non-privileged accounts.

B.17.3 SC-3 SECURITY FUNCTION ISOLATION

Interview

Does the system isolate all security functions from non-security functions?

How does the system isolate security functions from non-security functions?

Does the system maintain a separate execution domain (e.g., address space) for each executing process?

Examine

Review relevant system documentation to determine whether the organization defines the security functions of the system to be isolated from non-security functions.

Test

Observe the design of the system and functionality of system components as installed, as well as access enforcement mechanisms, to confirm that the system isolates security functions from non-security functions.

Work with the ISSO and system team as necessary to obtain a walk-through test of each system interface and user console or client, accessing those interfaces in real time as both an end-user and privileged user. Note the key differences. Verify information security function management is not available to end-users or any roles not authorized to manage security. Inspect the functionality of each interface, or console, using the example accounts, and verify the system enforces adequate separation of end-user functionality from system security (management) functionality.

B.17.4 SC-4 INFORMATION IN SHARED RESOURCES

Interview

How does the system prevent unauthorized and unintended information transfer via shared system resources?

Examine

Review relevant system documentation to determine whether the system prevents unauthorized and unintended information transfer via shared system resources.

Test

Work with the ISSO and system administrator team as necessary to obtain a walk-through demo of the systems functionality of system components, including any automated access enforcement mechanisms, that are implemented to prevent any unauthorized and unintended information transfer via shared system resources. Inspect and observe the controls in place to verify that the controls demonstrated (such as system procedures and configuration access and/or encryption settings) provide adequate capabilities to protect NRC data present in any shared system resources as per this control and related NRC-defined policies and standards.

B.17.5 SC-5 DENIAL OF SERVICE PROTECTION

Interview

How does the system protect against the NRC defined types of denial of service attacks?

Examine

Review relevant system documentation to determine whether the system implements mechanisms to protect against or limit the effects of denial of service (DoS) attacks.

Test

Work with the ISSO and system administrator team as necessary to arrange for a scan of the system using NRC approved scanning tools and scan types able to test the system for any DoS vulnerabilities or risks. Ensure that only an instance of the system approved for DoS testing is used. Verify that the scanners DoS testing methods are enabled. Working with the scanner and test results confirm that the system's mechanisms in place are able to protect against or limit the effects of denial of service attacks to ensure that system implements such mechanisms as documented in system documentation and in accordance with NRC defined requirements.

B.17.6 SC-7 BOUNDARY PROTECTION

Interview

What are the key internal and external boundaries of the system? Where are these boundaries documented?

How does the system monitor and control communications at the external boundary of the system and at key internal boundaries within the system?

Do system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site?

Examine

Review relevant system documentation to determine whether the system:

- Defines the external boundary of the system; and
- Defines key internal boundaries of the system.
- Review system configurations to ensure that the system implements sub networks for publicly accessible system components in accordance with NRC defined requirements

Test

Work with the ISSO and system administrator team to inspect and observe the system's boundary protection devices, as applicable, including their logical location within the system, to verify that the system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.

Inspect and verify that the system architecture and topology to confirm that the system connects to external networks or systems only through managed interfaces consisting of boundary protection devices, as per this control and NRC requirements.

Work with the ISSO and system administrator team as necessary to arrange for scanning tests and/or the use of the router and/or switch audit tools necessary (using NRC authorized tools) to verify that the system's automated mechanisms used to provide boundary protection security are in place and working as required, protecting each of the system's interfaces per NRC-defined requirements and this security control.

Enhancement 3

Interview

How has the organization limited the number of access points to the system of inbound and outbound network traffic?

What are the access points that allow inbound and outbound network traffic?

Examine

Review relevant system documentation to determine whether the organization limits the number of external network connections to the system.

Test

Work with the ISSO and system administrator team as necessary to arrange for scanning tests (using NRC authorized tools) to verify that the system's automated mechanisms implemented to provide boundary protection security are in place and working as required, limiting the number of external network connections to the system for each interface as per NRC-defined requirements and this security control. Note: Many scanning or anti-DoS test tools are able to test for excess connection handling vulnerabilities (a type of Denial of Service vulnerability) when configured to do so.

Enhancement 4

Interview

Have security controls (i.e., boundary protections devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service been defined?

Has a managed interface with any external telecommunication service been implemented?

Have controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted been implemented?

Examine

Review relevant system documentation to ensure that the organization:

- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need, and that the organization reviews exceptions to the traffic flow policy in accordance with the NRC defined frequency; and

- Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted.

Test

Work with the system's ISSO and system administrator team to access and inspect any of the system's managed interface(s) for external telecommunication services to verify that the organization establishes an appropriate traffic flow policy for each managed interface that satisfies NRC-defined policies and requirements of this control. Check any logs the interface device maintains for abnormal security conditions or errors.

Work with the system's ISSO and system administrator team to access and inspect the configurations of the managed interface(s) for external telecommunication services to ensure that the system protects the confidentiality and integrity of the information being transmitted across each interface. Verify that any cryptographic mechanisms used to protect the confidentiality of telecommunication information are FIPS-140-2 validated. Check any logs the interface device maintains for proper operation or abnormal security conditions or errors.

Enhancement 5

Interview

Does the system deny network traffic by default and allow network traffic by exception (i.e., deny all, permit by exception)?

How does the system deny network traffic by default and allows network traffic by exception?

Examine

Review relevant system documentation to determine whether for both inbound and outbound network communications traffic, the system implements a deny all, permit by exception network communications traffic policy.

Test

Work with the ISSO and system administrator team as necessary to arrange to access and inspect the configuration files of the system's boundary protection devices to ensure that for both inbound and outbound network communications traffic, the system enforces a deny all, permit by exception network communications traffic policy. Note: To simplify and aid this testing, if feasible, most firewalls and routers or boundary protection devices can be tested with common scanners and/or vendor provided or 3rd party automated firewall or router auditing tools if/where approved by the NRC.

Work with the system's ISSO and system administrator team to access, inspect and where feasible scan or test the system's boundary protection devices to verify that the organization enforces an appropriate a deny all, permit by exception network communications traffic policy in-place within each boundary protection device. Check any logs the interface device maintains for abnormal security conditions or errors.

Enhancement 7

Interview

How does the system prevent devices connecting remotely from simultaneously establishing non remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling)?

Examine

Review relevant system documentation to determine whether the system prevents devices connecting remotely from simultaneously establishing non remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).

Test

Work with the system's ISSO and system administrator team to access, inspect the current in-place configurations of the system's boundary protection devices to verify that the system prevents any devices connecting remotely from simultaneously establishing non remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).

Work with the system's ISSO and system administrator team to arrange for a hands-on split-tunneling test as applicable. Using an agreed upon client or system server able to access a VPN bring up the necessary network connection monitoring consoles or tool on the system. Establish a VPN connection. Note the VPN connection should now be the only one available. Attempt to establish another outbound external test (non-VPN) connection to the Internet or another system. The attempt to create an added connection should fail or cause the VPN to disconnect. The system should not be able to act as a form of router between two or more external systems.

Enhancement 8

Interview

Does the system route internal communications traffic to external networks through authenticated proxy servers in accordance with NRC policy?

Examine

Review relevant system documentation to determine whether the system routes NRC defined internal communications traffic to NRC defined external networks through authenticated proxy servers.

Test

Work with the system's ISSO and system administrator team to access and inspect the applicable system boundary protection and network devices, including their logical location with the system, and inspect or test the system configurations to verify that the system routes NRC defined internal communications traffic to NRC defined external networks through authenticated proxy servers. Inspect the devices current or recent traffic logs to verify the required routing is taking place. Note: Many devices can be tested or audited and inspected by automated tools the vendor of the NRC-approved device provides. Or another NRC-authorized 3rd party tool might be used for testing and auditing the device.

Enhancement 18

Interview

Do boundary protection devices fail securely in the event of an operational failure?

Examine

Review relevant system documentation to determine whether boundary protection devices should fail securely in the event of an operational failure.

Review relevant system architecture and design to determine whether boundary protection devices should fail securely in the event of an operational failure.

Test

Work with the system's ISSO and system administrator team to access and inspect any automated mechanisms the system uses to support and/or provide secure failure of the system in the event the system's boundary protection devices or mechanisms fail. Inspect and verify that the in-place current configurations of boundary protection devices will ensure the devices fail securely (not open or in any "bypass" mode) in the event of an operational failure. The devices logs might be inspected to help verify whether the device has failed recently and what state it entered into. Also the system's network monitoring mechanisms might be queried to see what status the system was left in, secure or vulnerable to any connections, if or when the devices failed in the past.

Enhancement 21

Interview

What are the different missions and/or business functions that the system supports?

Does the system isolate system components performing different missions and/or business functions in accordance with NRC defined requirements?

Examine

Review relevant system documentation to determine:

- The different missions and/or business functions that the system supports; and
- Whether the system isolates system components performing different missions and/or business functions in accordance with NRC defined requirements.

Test

Work with the system's ISSO and system administrator team to access and inspect the current in-place configurations of boundary protection devices to verify that the system isolates system components performing different missions and/or business functions in accordance with NRC defined requirements. The device's traffic logs might be checked to verify how the device actively manages the segregated traffic. Also the system's network monitoring mechanisms or tools might be used to visually identify what network interfaces or segments the device(s) actually route segregated traffic to, verifying whether the network isolations and communications meet the authorized system design and NRC policies.

B.17.7 SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Interview

How does the system protect the confidentiality and integrity of transmitted information?

Examine

Review relevant system documentation to determine the mechanisms used to protect the confidentiality and integrity of transmitted information.

Test

Work with the system's ISSO and system administrator team to access and inspect and/or scan with NRC-approved tools the current in-place mechanisms the system uses to protect the confidentiality and integrity of transmitted information. Verify that any cryptographic mechanisms used are FIPS140 2 validated. Many such devices may also be tested for these characteristics with NRC approved scanners.

Enhancement 1

Interview

Are cryptographic mechanisms used in the system to prevent unauthorized disclosure of information and/or recognize changes to information during transmission? If so, what are the cryptographic measures used?

Are alternative physical measures used to protect the confidentiality and integrity of transmitted information? If so, what are the alternative physical measures?

Examine

Review relevant system documentation to determine whether the system:

- Employs cryptographic mechanisms to prevent unauthorized disclosure of information and/or recognize changes to information during transmission.
- Employs alternative physical measures to protect the confidentiality and integrity of information during transmission.

Test

Observe the mechanisms used to protect the confidentiality and integrity of transmitted information to ensure that system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information in accordance with NRC defined requirements during transmission unless otherwise protected by NRC defined alternative physical safeguards. – OR -

Work with the system's ISSO and system administrator team to identify and inspect any alternative physical safeguards in place for the system used to restrict access to the network communications links and data intended to prevent unauthorized access, snooping, captures, or changes to the data and sessions being communicated. Verify that these alternate network safeguards satisfy NRC-defined security requirements and this control.

B.17.8 SC-10 NETWORK DISCONNECT

Interview

What is the time period of inactivity before the system terminates a network connection?

Does the system terminate a network connection at the end of a session or after the end of the time period of inactivity?

Examine

Review relevant system documentation to determine whether the system terminates network connections associated with a communications session at the end of the session or after the NRC defined period of inactivity.

Test

Inspect the system's active configurations to ensure the system is setup to terminate network connections associated with a communications session at the end of the session or after the NRC defined period of inactivity.

Work with the system's ISSO and system administrator team to identify, inspect, and observe a network communications session with each system interface. Verify that each interface does successfully terminate any sessions witnessed as described in system documentation and in accordance with NRC defined requirements.

B.17.9 SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Interview

What automated mechanisms are used to establish and manage cryptographic keys?

Do these mechanisms have supporting procedures or manual procedures?

What are the procedures called and where can they be found?

Examine

Review relevant system documentation to determine whether the organization establishes and manages cryptographic keys for required cryptography employed within the system in accordance with NRC defined requirements.

Test

For all applicable components, work with the system's ISSO and system administrator team to identify, inspect, and observe each process the system may use for generating cryptographic keys to verify that keys are generated in accordance with NRC defined requirements.

For all applicable components, work with the system's ISSO and system administrator team to request a walk-through of and observe the process for distributing cryptographic keys on the system to verify that keys are actually distributed in accordance with NRC defined requirements.

Observe the mechanisms and/or processes used for storing cryptographic keys on the system to verify that keys are stored in accordance with NRC defined requirements.

Inspect and verify that only approved trust anchors (e.g., root certificates) are stored in the system.

For all applicable components, work with the system's ISSO and system administrator team for a walk-through to inspect and observe the access control mechanisms for storing cryptographic keys to verify that only authorized personnel are provided access to key management functionality in accordance with NRC defined requirements. Inspect the access control list in effect for the locations the keys are stored in and verify the list is current with only the appropriate NRC-required users, access rights, and permissions.

Arrange with the system's ISSO and system administrator team for a walk-through of and observe the process they use for destroying cryptographic keys on the system to ensure keys are destroyed in accordance with NRC defined requirements.

Enhancement 1

Interview

How does the system maintain availability of information in the event of the loss of cryptographic keys by users?

Examine

Review relevant system documentation to determine whether the system maintains availability of information in the event of the loss of cryptographic keys by users.

Test

Work with the system's ISSO and system administrator team to understand, access, and inspect the mechanisms (e.g., key escrow) used to maintain the availability of information in the event of the loss of cryptographic keys by users.

Work with the system's ISSO and system administrator team to request a walk-through of and observe authorized system personnel demonstrate the use of their process and any automated mechanisms and/or tools used to recover information in the event of the loss of cryptographic keys by users (e.g., user forgets the passphrase). A test scenario or exercise may be arranged where the team recovers a test user account or folder with "lost keys" may be used for testing and to confirm that authorized staff can use it.

B.17.10 SC-13 CRYPTOGRAPHIC PROTECTION

Interview

Does the information processed, stored, or transmitted by the system require cryptographic protection?

Does the implementation of cryptographic protection in the system comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance?

Examine

Review relevant system documentation to determine whether the system implements cryptographic mechanisms in accordance with NRC defined requirements and applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Test

Arrange with the ISSO and system administrator team to scan or test and inspect all system components that use cryptographic mechanisms as needed to verify that they are implemented in accordance with NRC defined requirements and applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Verify that all uses of cryptographic mechanisms are FIPS-140-2 validated and operating in FIPS-mode.

B.17.11 SC-15 COLLABORATIVE COMPUTING DEVICES

Interview

Does the system prohibit remote activation of collaborative computing mechanisms? If so, how?

Does the system have the ability to provide an explicit indication that collaborative computing mechanisms are in use to the local users? If so, how does the system provide this indication?

Examine

Review relevant system documentation to determine whether the system:

- Prohibits remote activation of collaborative computing devices in accordance with NRC defined requirements; and
- Provides an explicit indication of use to users physically present at the devices.

Test

Work with the system team to locate and inspect the current in-place system inventory comparing with the system's authorized architecture and topology and configuration to verify that any collaborative computing devices (e.g., networked white boards, cameras, microphones, etc.) are not used on the system except in accordance with NRC defined exceptions.

Work with the system team to locate, demonstrate, and observe collaborative computing devices used within the system to ensure that they provide an explicit indication of the device's being activated or in use to users physically present near or at the devices (e.g., a light or signal that indicates that a microphone is active). Verify that the devices behave as required by NRC-defined requirements and this control.

B.17.12 SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Interview

How are public key infrastructure certificates issued?

Examine

Review relevant system documentation to determine how public key infrastructure certificates are issued.

Test

Work with the system's ISSO and system administrator team to request a walk-through of and observe the process they use to issue public key certificates or to obtain public key certificates from an NRC-approved service provider to ensure that public key certificates are issued in accordance with NRC defined requirements.

B.17.13 SC-18 MOBILE CODE

Interview

What are the usage restrictions and implementation guidance for the use of mobile code technologies?

Do the usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations?

Was this guidance based on the potential to cause damage to the system if used maliciously?

Who is responsible for authorizing, monitoring, and controlling the use of mobile code within the system?

How is the mobile code authorized, monitored, and controlled?

Do the mobile code control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the system?

Examine

Review relevant system documentation to determine whether the system:

- Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the system if used maliciously; and
- Authorizes, monitors, and controls the use of mobile code within the system.

Test

Work with the system's ISSO and developer team as necessary to identify and Examine what mobile code technologies are included in the system or application. Access and inspect the applicable system or application components and their properties with the developers and/or ISSO to verify that only acceptable mobile code technologies or types are used on the system as described in system documentation and in accordance with NRC defined requirements.

Working with the developers or system team as necessary to inspect the versions of mobile code technologies in-place to ensure that the latest versions are being used, and that outdated versions have been removed. Note: Where NRC-approved source-code security testing and scanning tools may be available these can often be used to collect and verify all the necessary details on the mobile code objects used.

B.17.14 SC-19 VOICE OVER INTERNET PROTOCOL

Interview

Does the system employ VoIP technology?

What are the usage restrictions and implementation guidance for VoIP technologies?

Was the guidance based on the potential to cause damage to the system if used maliciously?

Who is responsible for authorizing, monitoring, and controlling the use of VoIP within the system?

How is the use of VoIP within the system authorized, monitored, and controlled?

Examine

Review relevant system documentation to determine whether the system establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the system if used maliciously.

Test

Work with the ISSO and/or system team as necessary to obtain a walk-through of and inspect the configurations of VoIP management devices in the system as well as applicable boundary protection devices to verify that any VoIP components or implementations within the system are authorized, monitored, and controlled in accordance with NRC defined requirements.

Work with the system's ISSO and/or system team as necessary to receive a walk-through of any VoIP mechanisms or components in the system. Walk through the organizational process used for authorizing, monitoring, and controlling their VoIP implementation, including their use of any automated mechanisms or consoles and tools that support and/or implement, authorize, monitor, and control their VoIP system or components. Verify that all the NRC-defined security requirements applicable to their VoIP implementation and configuration are met, including if managed by 3rd parties.

B.17.15 SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Interview

What name/address lookup service is provided by the system?

Does this service allow entities to access organizational information resources across the Internet?

Does it provide artifacts for additional data origin authentication?

Are data integrity artifacts along with the authoritative data returned in response to resolution queries?

Examine

Review relevant system documentation to determine whether the system:

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

Test

Work with the system's ISSO and/or system team as necessary to receive a walk-through of and inspect the name/address resolution service configurations on the system, and run test Domain Name System (DNS) queries. Verify that the system provides additional data origin and integrity artifacts (such as DNS Security Extensions [DNSSEC]) digital signatures and cryptographic keys) along with the authoritative name resolution data the system returns in response to external name/address resolution queries. The system may be test-queried with DNS resolver clients to verify that this information is received by the client.

Work with the system's ISSO and/or system team as necessary to receive a walk-through of and inspect the name/address resolution services on the system. Verify that the system 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, if/when operating as part of a distributed, hierarchical namespace. Test DNS queries may be executed to verify secure DNS status, and/or use the system's DNS consoles to view domains, etc.

B.17.16 SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Interview

What name/address resolution service is provided for local clients?

Does this service perform data origin authentication?

Is there a data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems?

Examine

Review relevant system documentation to determine whether the system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Test

Work with the system's ISSO and/or system team as necessary to access and inspect the system's DNS services console and status details. Access and observe the system's DNS consoles or tools for inspecting or testing the name/address resolution services on the system to verify that each client of name/address resolution services on the system requests and performs data origin authentication and data integrity verification using the name/address resolution responses the system receives from authoritative sources, as per NRC-defined requirements applicable to the system.

B.17.17 SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Interview

How does the name/address resolution service implement fault tolerance and role separation?

Examine

Review relevant system documentation to determine whether name/address resolution services are fault tolerant and implement internal/external role separation.

Test

Work with the system’s ISSO and/or system team as necessary to access and inspect the system’s DNS services configuration, services, and active architecture. If the system collectively provides name/address resolution service for the organization, inspect and verify the configurations and implementation of name/address resolution components and services on the system are fault tolerant and implement internal/external role separation. The DNS service provider’s consoles and tools may often be used to directly view and verify DNS service status including fault tolerance. If possible the system team may be able to demonstrate how their DNS responds in a fault condition.

B.17.18 SC-23 SESSION AUTHENTICITY

Interview

What mechanisms are in place to protect the authenticity of communications sessions?

Examine

Review relevant system documentation to determine whether the system protects the authenticity of communications sessions.

Test

Work with the system’s ISSO and/or system team as necessary to get a walk-through of and inspect any session authenticity mechanisms used on the system (such as a challenge response authentication mechanism) to verify that the system protects the authenticity of communications sessions, and per NRC-defined policies.

B.17.19 SC-24 FAIL IN KNOWN STATE

Interview

When system components fail, do they preserve system state information and fail to system failure states?

Examine

Review relevant system documentation to ensure the organization has defined known system failure states in accordance with NRC defined requirements.

Test

Work with the system's ISSO and/or system team as necessary to get a walk-through of and verify that the in-place system configurations intended to ensure that upon failure, system components preserve their system state information and fail to secure system failure states as described in system documentation and in accordance with NRC defined requirements. Systems should not "fail-open" or in a bypass state where the security controls expected to be in place are not in effect and may be circumvented. In some cases NRC-approved scanning tools may assist with determining this status while the system or components are in the failed state.

B.17.20 SC-28 PROTECTION OF INFORMATION AT REST

Interview

What system components store information at rest?

How does the system protect information at rest?

Examine

Review relevant system documentation to determine:

- What system components store information at rest; and
- How the system protects information at rest.

Test

Work with the system's ISSO and/or system team as necessary to get a walk-through of and inspect the mechanisms used to protect information at rest to ensure that the organization protects the confidentiality and integrity of information at rest in accordance with NRC defined requirements. Check the properties and status of the security mechanisms or controls in effect at the time of the test.

Work with the system's ISSO and/or system team as necessary to get a walk-through of and verify the specific cryptographic mechanisms used to protect NRC information at rest and verify they are implemented in accordance with NRC defined requirements, FIPS-140-2, and applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Many NRC-approved system and network scanning tools can also be used to verify that all uses of cryptographic mechanisms on the system are FIPS-140-2 validated and operating in FIPS-mode.

B.17.21 SC-39 PROCESS ISOLATION

Interview

Does the system maintain a separate execution domain for each executing process?

Examine

Review relevant system documentation to determine whether the system is configured to maintain a separate execution domain for each executing process.

Examine the relevant system properties for the OS or application to confirm that the system is in fact configured to provide process isolation per NRC-defined standards.

Test

Work with the system ISSO and system administrator team as necessary to understand what process memory space isolation controls are used by the system. Work with the team to test the automated mechanisms supporting and/or providing separate execution domains for each executing process (as through 3rd party "sandbox" tools like Uhuru for Windows; or "cgroups" for Linux). For example either the systems installed 3rd party utilities console or tools may be used if adequate to determine the status of the process isolation, or a 3rd party process monitoring Graphical User Interface (GUI) tools might be used to test active processes and settings. Confirm that the system is operating with the NRC-defined level of process isolation.

B.18 SYSTEM AND INFORMATION INTEGRITY (SI)

System and information integrity assessment objects include, but are not limited to: policy and procedures; vulnerability assessment report; periodic scan report; system change requests; and tasks performed by organization staff in support of system and information integrity functions.

B.18.1 SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Interview

Are system-specific system and information integrity procedures available?

Who is responsible for reviewing, updating, and disseminating the procedures?

How are they disseminated? Are there records to support that they were disseminated?

How often are the procedures reviewed and updated?

Are there records to support that reviews and updates took place?

Examine

Review the system policy to determine:

- Whether the policy addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, consistent with the organization's mission and functions and compliant with applicable laws, directives, policies, regulations, standards, and guidance.
- Whether the system policy aligns with NRC policy.

Review the system procedures to determine whether they facilitate the implementation of the policy and associated system and information integrity controls.

Examine organization records to determine whether the policy and procedures were reviewed and updated per the NRC required frequency as stated in CSO-STD-0020.

Review the policy and procedures to determine whether they identify the organization elements that they must be disseminated to, and whether the elements include NRC defined personnel.

Examine organization records to determine whether or not policy and procedures were disseminated to the NRC defined personnel.

Review the system-specific system and information integrity policy and procedures to determine whether they are documented, reviewed, and updated in accordance with the requirements described in CSO-PROC-2104, “System Artifact Examination Procedure.”

B.18.2 SI-2 FLAW REMEDIATION

Interview

Does your organization identify, report, and correct system flaws? If so, how?

Who is responsible for identifying the flaws?

Who is responsible for reporting the flaws? Who are the flaws reported to?

Who is responsible for correcting the flaws?

Does your organization have a process for installing software and firmware updates related to flaw remediation on the system? If so, is the process documented?

Does your organization test software and firmware updates related to flaw remediation before installing them?

How often are the updates installed?

Are all flaw remediation updates tracked as part of the system’s configuration baseline?

Examine

Review vulnerability assessment reports, periodic scan reports, or other relevant system and information integrity documentation to verify that the organization identifies, reports, and corrects system flaws.

Review change requests or other records of flaw remediation to verify that the organization:

- 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 the NRC defined time period] of the release of the updates; and
- Incorporates flaw remediation into the organizational configuration management process.

Enhancement 1

Interview

How is the flaw remediation process managed?

Who is responsible for planning and implementing flaw remediation security controls?

Who is responsible for assessing, and monitoring flaw remediation security controls?

Who is responsible for authorizing flaw remediation security controls?

Examine

Review relevant system documentation to determine whether the flaw remediation process is implemented as described by system documentation and in accordance with NRC defined requirements.

Observe Examine any mechanisms used to centrally manage the flaw remediation process to ensure the flaw remediation process is implemented as described by system documentation and in accordance with NRC defined requirements.

Test

Work with the ISSO and system administrator team as needed to arrange to observe and confirm through demonstration that authorized system personnel manage the flaw remediation process, mechanisms, and tools per NRC-defined requirements and this control.

Enhancement 2

Interview

Does your organization use automated mechanisms to determine the flaw remediation state of your system? If so, please describe the mechanisms. How often do the mechanisms test and report the flaw remediation status of the system?

Examine

Review the results or scan reports from the most recent scan to ensure the organization determines the state of flaw remediation in accordance with the NRC defined frequency.

Review the automated mechanisms (i.e., scanners) used to determine the state of system components with regard to flaw remediation to confirm that the mechanisms have been approved by the NRC.

Test

Work with the ISSO as necessary to access, view, and Examine the automated mechanisms (i.e., scanners) console and scanning logs or history. Via the information in the logs or history, confirm that the flaw remediation capability has been tested and reports the system’s components flaw remediation status on an NRC approved frequency and using NRC approved methods.

B.18.3 SI-3 MALICIOUS CODE PROTECTION

Interview

Does the system implement malicious code protection? If so, are malicious code protection solutions implemented? Are different products from different vendors used?

Where are malicious code protection mechanisms implemented?

How often are the mechanisms updated? Who is responsible for updating them?

How are the mechanisms configured?

How often do the mechanisms scan the system for malicious code?

Are real time scans supported?

What events prompt a real time scan?

What happens when malicious code is detected?

How are false positives identified? How are they handled?

Examine

Review relevant system documentation to determine whether the system employs malicious code protection mechanisms in accordance with NRC defined requirements.

Examine the malicious code protection mechanisms used on the system to ensure they have been approved by the NRC.

Review the configurations of malicious code protection mechanisms to ensure that the system performs periodic scans of the system in accordance with the NRC defined frequency.

Examine the configurations of malicious code protection mechanisms to ensure that the system conducts real time scans of files from external sources as the files are downloaded, opened, or executed in accordance with NRC defined requirements.

Review the configurations of malicious code protection mechanisms to ensure that the system automatically responds to malicious code in accordance with NRC defined requirements.

Test

Work with the ISSO and/or system administrator team as necessary to run through a test pass using the organizational processes used for deploying, configuring, and updating malicious code protection mechanisms on the system, such as by redeploying the anti-virus client to a test system. Confirm the processes successfully deploy and configure and can update the mechanisms per NRC-defined requirements;

Run through a test pass of any automated mechanisms supporting and/or implementing the deployment, updating, and configuring of malicious code protection mechanisms to confirm they operate as expected and configure the mechanisms to meet NRC-defined policies and requirements; -OR-

Run through a test pass of any automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions. –OR-

Run through a test pass of any organizational process (automated and/or manual) for addressing false positives and resulting potential impact.

Enhancement 1

Interview

How are the malicious code protection mechanisms managed?

Who is responsible for planning and implementing malicious code protection security controls?

Who is responsible for assessing, and monitoring malicious code security controls?

Who is responsible for authorizing malicious code security controls?

Examine

Review relevant system documentation to determine whether the system employs a mechanism for centrally managing malicious code protection mechanisms in accordance with NRC defined requirements.

Test

Inspect the mechanism (i.e., console or tool) used to centrally manage malicious code protection mechanisms to confirm that the malicious code protection mechanisms are implemented as described by system documentation and in accordance with NRC defined requirements.

Enhancement 2

Interview

Does the system automatically update malicious code protection mechanisms? If so, how?

Examine

Review relevant system documentation to determine whether the system automatically updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.

Test

Examine the update logs and settings of the malicious code protection mechanisms to verify the malicious code protection mechanisms are automatically updated whenever new releases are available and are current in accordance with NRC and organizational configuration management policy and procedures.

B.18.4 SI-4 INFORMATION SYSTEM MONITORING

Interview

Does your organization monitor the system to detect attacks (and potential attacks) and unauthorized local, network, and remote connections? If so, how, and how often?

Where are the monitoring devices deployed within the system?

Is the information obtained by monitoring devices protected from unauthorized access? If so, how?

Under what circumstances would your organization monitor the system more frequently, or in greater detail?

Has your organization obtained a legal opinion concerning the monitoring activities?

What information is reported concerning monitoring activities? Who is it reported to? How often is it reported?

Examine

Review relevant system documentation to determine whether the organization monitors the system in accordance with NRC defined requirements.

Test

Work with the ISSO and system administrator team as needed to arrange for a network based test scan (such as for vulnerabilities) of the system while being monitored. Log into and observe the performance of the system monitoring devices used to verify that the system detects attacks and indicators of potential attacks as well as attempted unauthorized local, network, and remote connections in accordance with NRC defined requirements. Any NRC approved scanning or pen-testing tool used to scan a system for vulnerabilities should generate enough of these kinds of packets to trigger the monitoring system to log and capture much of the scanner traffic as suspicious, etc.

Observe the system monitoring devices while in use to ensure the system identifies attempts to obtain unauthorized use of the system (such as from scanning or pen-testing tools, simple failed login attempts, unauthorized devices or computers etc., misuse of ports or services etc.) in accordance with NRC defined requirements.

Examine system monitoring devices implementations, including their logical location with the system, to verify the devices are deployed strategically within the system (such as at appropriate perimeter locations) to collect adequate organization determined essential information and at ad hoc locations within the system to track specific types of higher value or risk transactions of increased interest to the organization.

Work with the ISSO and system administrator team as needed to test the access to the system monitoring devices access enforcement mechanisms to verify that information obtained by and stored in the intrusion monitoring tools is protected from unauthorized access, modification, and deletion. Only users authorized to access the organization's intrusion-monitoring tools should be able to access this information, as per NRC requirements.

Enhancement 2

Interview

Does your organization use automated tools to support near real time analysis of events? If so, please describe the tools and their capabilities.

Examine

Review relevant system documentation to determine whether the system is capable of near real time analysis of events.

Test

Work with the ISSO and system administrator team as needed to access and use the system's automated tools that support system monitoring. Verify that the tools are capable of near real time analysis of events captured by the monitoring tools.

Enhancement 4

Interview

Does your organization monitor inbound and outbound communication traffic for unusual or unauthorized activities or conditions? If so, how often?

Examine

Review relevant system documentation to determine whether the system monitors inbound and outbound communications traffic in accordance with the NRC defined frequency for unusual or unauthorized activities or conditions.

Test

Work with the ISSO and system administrator team as necessary to arrange for automated test scanning of the system with all the system's normal security protections enabled. This testing is only intended to confirm that system monitoring itself is working. While scanning is taking place observe the system's monitoring mechanisms in operation to verify that the tools monitor both inbound and outbound communications traffic in accordance with the NRC defined frequency for unusual or unauthorized activities or conditions.

View the monitoring tool's traffic consoles and/or logs as appropriate to verify the tools are functioning effectively without failures or significant errors and are properly logging any suspicious, unusual, or unauthorized traffic on the NRC-defined frequency.

Enhancement 5

Interview

Does the system alert personnel if specific issues are identified that suggest the system has been or could potentially be compromised? If so, what issues trigger an alert? Who is alerted?

Examine

Review relevant system documentation to determine whether the system automatically alerts NRC defined personnel in accordance with NRC defined requirements.

Test

Work with the system ISSO and system administrator team as necessary to understand its alerting and notification capabilities as implemented. Arrange an agreed upon test of those capabilities setting off a set of agreed upon alert triggers (a matching non-production test system may be used if similarly configured). Observe the system's monitoring devices as they are triggered to verify they automatically alert NRC defined personnel in accordance with NRC defined requirements.

B.18.5 SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Interview

Are external organizations from whom information system security alerts, advisories, and directives are received identified? If so, where are they identified?

Are information system security alerts, advisories, and directives received from organization-defined external organizations on an ongoing basis? If so, where are they stored?

Are internal security alerts, advisories, and directives issued from the external organization security alerts, advisories, and directives as deemed necessary? If so, how are they issued? Are they stored somewhere? If so, where?

Are personnel or roles to whom security alerts, advisories, and directives are to be provided identified? If so, where are they identified?

Are external organizations to whom security alerts, advisories, and directives are to be provided identified? If so, where are they identified?

Examine

Review relevant documentation to determine:

- If external organizations from whom information system security alerts, advisories, and directives are received identified;
- If information system security alerts, advisories, and directives received from organization-defined external organizations are received on an ongoing basis;
- If and how internal security alerts, advisories, and directives issued from the external organization issued as security alerts, advisories, and directives as deemed necessary;
- If personnel or roles to whom security alerts, advisories, and directives are to be provided identified;
- If external organizations to whom security alerts, advisories, and directives are to be provided identified;
- If security alerts, advisories, and directives are distributed to one or more of the following:
  - ✓ organization-defined personnel or roles;
  - ✓ organization-defined elements within the organization; and/or
  - ✓ organization-defined external organizations; and
- If security directives are implemented in accordance with established time frames

Enhancement 1

Interview

Does your organization employ automated mechanisms to make security alert and advisory information available throughout the organization. If so, please describe the tools and their capabilities.

Examine

Review relevant system documentation to determine whether the system is capable of employing automated mechanisms to make security alert and advisory information available throughout the organization.

Test

Work with the ISSO and system administrator team as needed to access and use the system’s automated tools that support security alerts and advisories. Verify that the tools work as expected.

B.18.6 SI-6 SECURITY FUNCTION VERIFICATION

Interview

Does your organization verify the correct operation of NRC required security functions? If so, what are the functions, and how are they verified?

Who is responsible for verifying the functions?

When are the security functions verified?

Who is notified if a security function fails? Do records exist to demonstrate that the party was notified?

What actions are taken if a security function fails?

Examine

Review relevant system documentation to determine whether the system:

- Verifies the correct operation of NRC defined security functions;
- Performs this verification in accordance with NRC defined requirements;
- Notifies NRC defined personnel of failed security verification tests; and
- Takes the NRC defined actions when anomalies are discovered.

Test

Work with the ISSO and system administrator as required to understand and view the system’s security function verification mechanisms (i.e., tools that may track and monitor the status of NRC required security controls like anti-virus clients or end-point security clients and security policy settings) to confirm that these mechanisms do verify the correct operation of NRC defined security functions in accordance with NRC defined requirements.

Work with the ISSO and system administrator to execute and test the system’s security function verification mechanisms to confirm the mechanisms notify the correct NRC defined personnel whenever security verification test failures or security function anomalies occur on the system. Example security function tests may include actions such as manually stopping a certain monitored security function on a test client or server and then confirm the controls respond properly per NRC requirements.

B.18.7 SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Interview

Does your organization use integrity verification tools to detect unauthorized changes to the system? If so, specifically, what do the tools check (software, firmware, applications, system and user information)?

How do the tools detect and protect against unauthorized changes to software and information? What mechanisms are used?

Examine

Review relevant system documentation to determine whether the system detects unauthorized changes to software, firmware, and information in accordance with NRC defined requirements.

Test

Work with the system ISSO and system administrator staff to attempt changes on the system (such as a very similar test instance of). Observe the integrity checking mechanisms used to ensure the system detects unauthorized changes (successful or unsuccessful) to software, firmware, and information in accordance with NRC defined requirements.

Enhancement 1

Interview

When does your system perform the integrity checks?

Examine

Review relevant system documentation to determine whether the system performs an integrity check on NRC defined software, firmware, and information at startup and in accordance with other NRC defined events.

Test

Review system configurations and the configurations of integrity checking mechanisms to ensure that the system performs an integrity check on NRC defined software, firmware, and information at startup and in accordance with other NRC defined events.

Enhancement 2

Interview

Are organization personnel automatically notified if discrepancies are discovered during integrity checks? If so, who is notified?

Examine

Review relevant system documentation to determine whether automated integrity checking tools automatically notify NRC defined personnel upon discovering discrepancies during integrity verification.

Test

Review the configurations of automated integrity checking tools to ensure that the tools automatically notify NRC defined personnel upon discovering discrepancies during integrity verification.

Enhancement 5

Interview

What happens when integrity violations are discovered?

Examine

Review relevant system documentation to determine whether the system automatically responds to integrity violations in accordance with NRC defined requirements.

Test

Work with the ISSO and system administrator as required to test the system's automated integrity checking mechanisms to verify the system automatically responds to integrity violations in accordance with NRC defined requirements. Define an agreed to testing approach that may include deleting content and/or integrity hashes from test files that are monitored after including them in the tool's known system integrity monitoring baseline.

Enhancement 7

Interview

Does your organization track discovered integrity violations? If so, are they incorporated into your organization's incident response capability? How?

Examine

Review incident response documentation, change requests, or other relevant system and information integrity documentation to verify that the organization incorporates the detection of unauthorized NRC defined security relevant changes to the system into the organizational incident response capability.

Enhancement 14

Interview

Does your organization permit the use of binary or machine executable code? If so, under what conditions? Are the conditions documented and approved by an authorizing official? If so, who?

Examine

Review relevant system documentation to determine whether the system prohibits the use of binary or machine executable code from sources with limited or no warranty and without the provision of source code, except with the explicit written approval of the authorizing official (i.e., DAA).

Test

Work with the ISSO and system administrator as required to test the system's automated integrity checking mechanisms to ensure the system prohibits the use of non-NRC approved binary or machine executable code from sources with limited or no warranty and without the provision of source code, as per NRC policies, except with the explicit written approval of the authorizing official (i.e., DAA). Define an agreed-to testing approach that may include attempts to use binary or machine-executable test code that does not meet the NRC policy criteria above and verify the system blocks execution. If the automated hash or property checking of the binary does not prevent execution of the unauthorized binary or machine-code the test fails.

B.18.8 SI-8 SPAM PROTECTION

Interview

Does your organization use spam protection mechanisms? If so, where are the mechanisms located?

What actions do the mechanisms take when unsolicited messages are received?

How often does your organization update the spam protection mechanisms?

Examine

Review relevant system documentation to determine whether the organization :

- Prohibits the use of binary or machine executable code from sources with limited or no warranty and without the provision of source code; and
- Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the DAA.

Test

Work with the ISSO and system administrator as needed to inspect the spam protection mechanisms used on the system and its activity logs to ensure the mechanisms have been approved by the NRC and are deployed, and operating, at the appropriate system entry and exit points.

Exercise, using a spam filter test tools and test spam messages if possible, the spam protection mechanisms on workstations, servers, and mobile computing devices and the protection mechanism's filter logging on the network to ensure the spam filter detects and takes appropriate action on unsolicited messages (by sending test "SPAM" or unsolicited messages) transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means. Observe and document the results.

Using the system consoles to show running processes and the appropriate system and/or application event logs inspect the system for spam protection mechanism status and any significant error messages that may occur during its operation or testing.

Enhancement 1

Interview

How are the spam protection mechanisms managed?

Who is responsible for planning and implementing spam protection security controls?

Who is responsible for assessing and monitoring spam protection security controls?

Who is responsible for authorizing spam protection security controls?

Examine

Review relevant system documentation to determine whether the organization centrally manages spam protection mechanisms, whether the tasks and associated job roles called for above are defined, documented, and implemented, and how duties are assigned

Test

Request the system team (system administrator/ISSO) access the mechanism used to centrally manage the spam protection mechanisms. Ask them to demonstrate its use and functionality and observe to ensure that the spam protection mechanisms are implemented as described by system documentation and in accordance with NRC defined requirements.

Enhancement 2

Interview

Does your system automatically update spam protection mechanisms?

Examine

Review relevant system documentation to determine whether the system automatically updates spam protection mechanisms.

Test

Work with the ISSO and system team to access the system's anti-spam tools console or properties to verify the vendor's latest anti-SPAM pattern files have been downloaded and installed, and that the spam protection mechanisms automatically update spam protection mechanisms whenever new releases are available and in accordance with organizational configuration management policy and procedures.

B.18.9 SI-10 INFORMATION INPUT VALIDATION

Interview

Does your system validate system input? If so, how?

What does the system validate (e.g., character set, length, valid values).

In the event of an error with system input, what action does the system take?

Examine

Review relevant system documentation to determine whether the system checks the validity of NRC defined information inputs.

Test

Review system configurations to ensure that all user input is validated in accordance with NRC defined requirements.

If possible, observe a user entering invalid data into a field to ensure that system does not accept the input.

B.18.10 SI-11 ERROR HANDLING

Interview

Does your system generate error messages?

If so, what components of the system generate the messages? Are the messages reviewed prior to implementation to ensure that they do not reveal exploitable information to adversaries?

Are the error messages displayed only to specific personnel? If so, who?

Examine

Review relevant system documentation to determine whether the system:

- Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
- Reveals error messages only to NRC defined personnel or roles.

Test

Review system configurations to ensure that error messages on the system do not reveal exploitable information to adversaries.

If possible, observe a system error message to ensure that the system does not reveal exploitable information.

B.18.11 SI-12 INFORMATION HANDLING AND RETENTION

Interview

How does your organization handle and retain information within the system? How does your system handle and retain information output from the system?

Examine

Examine system and information integrity documentation to verify that the organization handles and retains information within the system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Test

Observe information stored on and generated by the system to ensure that the organization handles the information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Observe information stored on and generated by the system as well as information retention processes to ensure that the organization retains information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

B.18.12 SI-16 MEMORY PROTECTION

Interview

Does your system protect its memory from unauthorized code execution? If so, how?

Examine

Review system and information integrity documentation to determine whether the system implements NRC defined security safeguards to protect its memory from unauthorized code execution.

Test

Observe memory protection mechanisms, such as data execution prevention hardware or software, to ensure the system protects its memory from unauthorized code execution in accordance with NRC defined requirements.

APPENDIX C ASSESSMENT FINDING EXAMPLES

This appendix provides examples of the level of detail required when documenting assessment findings and supporting notes. The details required to support each finding (derived using the interview, examine, or test method) for each type of assessment object (specification, mechanism, or activity) are provided in Table 3.

Assessor notes must:

- Explain the finding within the context of the corresponding assessment method (interview, examine, or test) and assessment object (specification, mechanism, or activity).
- Provide the assessor’s rationale for the assessment finding in sufficient detail such that an individual who is not familiar with the system can easily arrive at the same conclusion that the assessor came to.
- Provide details in the rationale provided and evidence cited that are commensurate with the assurance requirements for the evaluated impact level to each supported security objective (confidentiality, integrity, and availability) as documented within the system’s security categorization (see NIST SP 800-53A for more details).
- Provide details for every applicable component of the system within the CSO approved sample selected for assessment.
- Cite supporting system artifacts that serve as a resource for understanding the implementation of the control.
- Identify system staff members who were interviewed or perform security related activities in support of security control implementation.
- For partially implemented security controls, indicate which portion of the control is implemented effectively, and the portion that is not implemented.

Per NIST SP 800-53A, the interview method should strictly be used to “facilitate assessor understanding, achieve clarification, or obtain evidence.” Statements made during interviews do not constitute evidence that a security control has been effectively implemented.

Table 3: Details Required to Support Assessment Findings

Finding	Details Required in Assessor Note
Satisfied Indicates that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result.	
Interview	**Specifications, Mechanisms, and Activities** The note must provide the role of the party Interviewed (e.g., system ISSO or system administrator), and a summary of the statement made concerning the specification, mechanism, or activity during the interview.
Examine	**Specifications** The note must provide the name of the document based system artifacts that were examined and the rationale for accepting each artifact as evidence that the control is implemented effectively. The rational must not simply state that the artifacts exist; it must

Table 3: Details Required to Support Assessment Findings

Finding	Details Required in Assessor Note
	explain how the artifact satisfies the intent of the supported security control.
	Mechanisms The note must identify the Examined mechanism (hardware, software, or firmware safeguards and countermeasures employed within the system), provide a brief description of the approach used to examine the mechanism, and provide a brief rationale for accepting the current implementation of the mechanism as evidence that the control is implemented effectively. The rationale must not simply state that the mechanism is in place; it must explain how the mechanism is implemented such that it satisfies the intent of the supported security control, and cite evidence of proper implementation.
	Activities The note must provide a brief description of the activity conducted (e.g., system backup operations, monitoring of network traffic, or exercising a contingency plan), identify the agency staff who conducted the activity (including their roles), and provide a brief rationale for accepting the activities as evidence that the control is implemented correctly. The rationale must not simply state that the activity takes place; it must explain whether the activity was observed by the assessor, logs were examined that indicated that the activity took place, or reports documented the outcome of the activity with the date that the activity took place.
Test	**Specifications** The note shall refer the reader to the note supporting the tested mechanism or activity.
	Mechanisms The note must identify the tested mechanism (hardware, software, or firmware safeguards and countermeasures employed within the system), provide a brief description of the approach used to test the mechanism, and provide a brief rationale for accepting the tested implementation of the mechanism as evidence that the control is implemented effectively. The rational must not simply state that the mechanism is in place; it must explain how testing indicates that the mechanism is implemented such that it satisfies the intent of the supported security control.
	Activities The note must provide a brief description of the activity conducted (e.g., flaw remediation, system patching, or configuring system components per agency standards), identify the agency staff who conducted the activity (including their roles), and provide a brief rationale for accepting the tested activities as evidence that the control is implemented correctly. The rationale must not simply state that the activity takes place; it must explain whether the activity was tested by the assessor, and provide a summary of the test outcome.
Other than Satisfied Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates potential anomalies in the operation or implementation of the control that may need to be addressed by the organization.	
Interview	Specifications, Mechanisms, Activities The note must include the role of the party interviewed (e.g., system ISSO or system administrator), and a summary of the statement made concerning the specification, mechanism, or activity during the interview.
Examine	**Specifications** The note must provide the name of the document based system artifact that was examined and a brief rationale for concluding that the artifact did not satisfy the intent of

Table 3: Details Required to Support Assessment Findings

Finding	Details Required in Assessor Note
	the supported security control. If the artifact does not exist, this must be stated. The note must also explain the potential impact to the security objectives supported by the specification (confidentiality, integrity, or availability). If the artifact does exist, the rational must not simply state that it does not satisfy the intent of the supported security control; it must briefly explain what was inaccurate, out of date, or lacking in detail sufficient to support the implementation of the control. The note must also explain the potential impact to the security objectives supported by the control (confidentiality, integrity, or availability). If an existing POA&M item is tracking the status of the POA&M, this must be stated in the note, and the weakness ID of the current POA&M item must be provided.
	Mechanisms The note must identify the Examined mechanism (hardware, software, or firmware safeguards and countermeasures employed within the system), provide a brief description of the approach used to examine the mechanism, and provide a brief rationale for determining that the current implementation of the mechanism is not effective. If the mechanism is not in place, or, the mechanism is in place, but is not implemented effectively, the rational must identify the issues that concern the assessor, and explain the potential impact to the security objectives supported by the control (confidentiality, integrity, or availability). If an existing POA&M item is tracking the status of the control implementation, this must be stated in the note, and the weakness ID of the current POA&M item must be provided.
	Activities The note must provide a brief description of the activity conducted (e.g., system backup operations, monitoring of network traffic, or exercising a contingency plan), identify the agency staff who conducted the activity (including their roles), and provide a brief rationale for determining that the activities are not conducted in a manner that satisfies the intent of the security control. The rationale must not simply state that the activity does not satisfy the intent of the security control; it must identify the issues that concern the assessor, and explain the potential impact to the security objectives supported by the activity (confidentiality, integrity, or availability). If an existing POA&M item is tracking the status of the control implementation, this must be stated in the note, and the weakness ID of the current POA&M item must be provided.
Test	**Specifications** The note shall refer the reader to the note supporting the tested mechanism or activity.
	Mechanisms The note must identify the tested mechanism (hardware, software, or firmware safeguards and countermeasures employed within the system), provide a brief description of the approach used to test the mechanism, and provide a brief rationale for determining that the tested implementation of the mechanism is not effective. If the mechanism is not in place, or, the mechanism is in place, but is not implemented effectively, the rational must identify the issues that concern the assessor, and explain the potential impact to the security objectives supported by the control (confidentiality, integrity, or availability). If an existing POA&M item is tracking the status of the control implementation, this must be stated in the note, and the weakness ID of the current POA&M item must be provided.

Table 3: Details Required to Support Assessment Findings

<table>
<tr><th>Finding</th><th>Details Required in Assessor Note</th></tr>
<tr><td></td><td><b>Activities</b>
The note must provide a brief description of the activity conducted (e.g., flaw remediation, system patching, or configuring system components per agency standards), identify the agency staff who conducted the activity (including their roles), and provide a brief rationale for determining that the activities are not conducted in a manner that satisfies the intent of the security control.
The rationale must not simply state that the activity does not satisfy the intent of the security control, the rational must identify the issues that concern the assessor, and explain the potential impact to the security objectives supported by the control (confidentiality, integrity, or availability).
If an existing POA&M item is tracking the status of the control implementation, this must be stated in the note, and the weakness ID of the current POA&M item must be provided.</td></tr>
<tr><td colspan="2"><b>Risk-based Decision</b>
Indicates that:
• The NRC DAA has accepted the risk associated with a deficient portion of a security control due to compensating controls and mitigating factors documented in a Deviation Request or Waiver Request per CSO-PROS-1324, “Deviation/Waiver Request Process,”
• The assessor believes that the driving factor for the deviation is still relevant
• The assessor believes that the risk accepted by the DAA continues to be consistent with the agency’s risk tolerance level.
• The assessor believes that compensating controls and mitigating factors are effectively implemented.
A signed deviation or waiver approval memo constitutes evidence that the NRC DAA has accepted the risk associated with the deficient assessment objective. However, when assessing security controls (or portions of controls) with approved deviations, if an approved deviation has expired, the driving factor is no longer relevant, the assessors believe the accepted risk is not consistent with the agency’s current risk tolerance level, or compensating controls are not effectively implemented, the associated security control must be assessed as Other than Satisfied.
If the assessors find the security control to be Other than Satisfied, the assessor note must identify the issues that concern the assessors, and explain the potential impact to the security objectives supported by the control (confidentiality, integrity, or availability).</td></tr>
<tr><td><b><i>Interview</i></b></td><td><b>Specifications, Mechanisms, Activities</b>
The note must include the role of the party Interviewed (e.g., system ISSO or system administrator), and a summary of the statement made concerning the specification, mechanism, or activity during the Interview.</td></tr>
<tr><td rowspan="2"><b><i>Examine</i></b></td><td><b>Specifications</b>
Development and maintenance of documented system artifacts is a federal and agency requirement. The DAA does not accept the risk associated with operating a system without required system artifacts.
If a required artifact is not developed, or is deficient, the associated security control must be assessed as Other than Satisfied, and the assessor note must identify the issues that concern the assessor, and explain the potential impact to the security objectives supported by the control (confidentiality, integrity, or availability).</td></tr>
<tr><td><b>Mechanisms</b>
The note must identify the mechanism and then indicate that the DAA has formally accepted the risk associated with operating the system without the mechanism. The note</td></tr>
</table>

Table 3: Details Required to Support Assessment Findings

Finding	Details Required in Assessor Note
	must provide the ADAMS accession number of the Deviation or Waiver Request and the signed DAA Approval Memo. The note must also indicate whether the driving factor for the deviation is still relevant, and whether the assessor believes that the risk associated with the deviation continues to be consistent with the agency's risk tolerance level. If compensating controls have been implemented, the assessor note must indicate that the implementation of the compensating control and mitigating factors remains effective.
	Activities The note must provide a brief description of the activity and then indicate that the DAA has formally accepted the risk associated with operating the system without conducting the activity. The note must provide the ADAMS accession number of the deviation or waiver request and the DAA Approval Memo. The note must also indicate whether the driving factor for the deviation is still relevant, and whether the assessor believes that the risk associated with the deviation continues to be consistent with the agency's risk tolerance level. If compensating controls have been implemented, the assessor note must indicate that the implementation of the compensating control remains effective.
Test	**Specifications** The note shall refer the reader to the note supporting the tested mechanism or activity.
	Mechanisms The note must identify the mechanism and then indicate that the DAA has formally accepted the risk associated with operating the system without the mechanism. The note must also provide the ADAMS accession number of the deviation or waiver request and the DAA approval memo. The note must also indicate whether the driving factor for the deviation is still relevant, and whether the assessor believes that the risk associated with the deviation continues to be consistent with the agency's risk tolerance level. If compensating controls have been implemented, the assessor note must indicate that the implementation of the compensating control remains effective.
	Activities The note must provide a brief description of the activity, explain that the organization has not conducted the activity, and then indicate that the DAA has formally accepted the risk associated with operating the system without conducting the activity. The note must also provide the ADAMS accession number of the deviation request or waiver request and the DAA approval memo. The note must also indicate whether the driving factor for the deviation is still relevant, and whether the assessor believes that the risk associated with the deviation continues to be consistent with the agency's risk tolerance level. If compensating controls have been implemented, the assessor note must indicate that the implementation of the compensating control remains effective.
Provided at agency Level Indicates that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control is provided at the NRC level for the system. CSO-STD-0021, "Common and Hybrid Security Control Standard," constitutes evidence that the assessment objective is provided at the NRC level by a common control provider. CSO-STD-0020, "Organization-Defined Values for System Security and Privacy Controls" constitutes	

Table 3: Details Required to Support Assessment Findings

Finding	Details Required in Assessor Note
evidence that a value is defined at the NRC level.	
Interview	**Specifications, Mechanisms, Activities** The note must include the role of the party Interviewed (e.g., system ISSO or system administrator), and a summary of the statement made concerning the specification, mechanism, or activity during the Interview.
Examine or Test	**Specifications, Mechanisms, Activities** The note must indicate that the specification, mechanism, or activity is provided by the common control provider identified in CSO-STD-0021, “Common and Hybrid Security Control Standard,” or that the value is defined in CSO-STD-0020.
Provided by <XYZ System> Indicates that for the portion of the security control addressed by a determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control is provided by system XYZ for the assessed system. A signed, currently effective service level agreement between the organizations providing and inheriting the assessment objective constitutes evidence that the assessment objective is provided as a service to the assessed system. Systems owned by the same organization are not required to have a service level agreement.	
Interview	**Specifications, Mechanisms, Activities** The note must include the role of the party Interviewed (e.g., system ISSO or system administrator), and a summary of the statement made concerning the specification, mechanism, or activity during the Interview.
Examine or Test	**Specifications, Mechanisms, Activities** The note must indicate that a signed, currently effective service level agreement is in place with another organization stating that the specification, mechanism, or activity is provided as a service by the other organization.
Not Applicable Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates that the assessment objective is not applicable to the assessed system per the scoping guidance provided in NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations.” For example, a security control that refers to a specific technology (e.g., wireless) is only applicable if wireless is employed within the assessed system.	
Interview	**Specifications, Mechanisms, Activities** The note must include the role of the party Interviewed (e.g., system ISSO or system administrator), and a summary of the statement made concerning the specification, mechanism, or activity during the Interview.
Examine or Test	**Specifications, Mechanisms, Activities** The note must indicate that the specification, mechanism, or activity is not applicable to the system because the associated technology is not employed.

C.1 Example: Assessment Finding of Satisfied

<table>
<tr><td colspan="2"><b>CM-2 – Baseline Configuration | Automation Support For Accuracy / Currency</b></td><td><b>Result: Satisfied</b></td></tr>
<tr><td colspan="3"><b>Assessment Method(s): Examine, Interview, Test</b></td></tr>
<tr><td>Objective ID</td><td>CM-2(2).1.1</td><td>Satisfied</td></tr>
<tr><td colspan="2">Determine if the organization employs automated mechanisms to maintain an up to date, complete, accurate, and readily available baseline configuration of the system.</td><td>Assessor Notes:
The <ABC> SSP states that the <ABC> system administrators update the baseline configuration as part of system component installations.
The assessor interviewed the system administrator, who stated that the <JKL> application serves as an automated mechanism for maintaining the system’s baseline configuration.
The assessor examined the <JKL> application and verified that<ABC> uses this application as an automated mechanism for maintaining the configuration baseline for the system. The configuration baseline is accurate and complete, and is updated at least annually or whenever a change is made to the system or in response to a security threat.</td></tr>
</table>

C.2 Example: Assessment Finding of Other than Satisfied

AC-7 – Unsuccessful Logon Attempts		**Result: Other than Satisfied**
Assessment Method(s): Examine, Interview, Test		
Objective ID	AC-7.1.2	Other than Satisfied
Determine if the system enforces the organization defined limit of consecutive invalid logon attempts by a user during the organization defined time period.		Assessor Notes: The ABC System Security Plan states that at the operating system level, the system is enforced to lock a user's <ABC> account after three invalid logon attempts in a 15 minute period. At the application level, the system locks a user's <JKL> application account after three unsuccessful logon attempts in a 15 minute period. Both accounts are locked for 30 minutes once the invalid logon attempt threshold is reached. The assessor Interviewed the system administrator, who confirmed that unsuccessful logon attempts are handled as described in the ABC System Security Plan. The assessor reviewed account lockout policies settings for account lockout policies for operating system accounts, <ABC> application accounts, and network device accounts. Basis for Other than Satisfied: The assessor found that the following network devices do not enforce account lockout after a certain number of invalid logon attempts: • <Network Device Hostname 1> • <Network Device Hostname 2> • <Network Device Hostname 3> Not enforcing an account lockout policy could allow an attacker to use brute force methods to gain unauthorized access to a system or device, compromising the confidentiality, and potentially the integrity and availability, of sensitive information.

C.3 Example: Assessment Finding of Risk-based Decision

<table>
<tr><th colspan="2">AU-8(1) – Time Stamps | Synchronization With Authoritative Time Source</th><th>Result: Risk-based Decision</th></tr>
<tr><td colspan="3"><b>Assessment Method(s): Examine, Test</b></td></tr>
<tr><td>Objective ID</td><td>AU-8(1).1.3</td><td>Risk-based Decision</td></tr>
<tr><td colspan="2">Determine if the organization synchronizes internal system clocks with the organization defined authoritative time source in accordance with the organization defined frequency.</td><td>Assessor Notes:
The <ABC> System Security Plan SSP states that the <ABC> NTP server is not configured to use an NRC authorized time source per CSO-STD-0020. <ABC> utilizes NIST approved time servers to synchronize timestamps on <ABC> servers.
<u>Basis for Risk-based Decision:</u>
The <ABC> NTP server is not configured to use the NRC authorized time source. A deviation request for the requirement to use the NRC authorized time source was submitted on August 1, 20XX (MLXXXXXXXXX); the request was approved by the DAA on September 1, 20XX (MLXXXXXXXXX). The deviation remains in effect until September 1, 20XX.
The assessor reviewed the approved deviation per CSO-PROS-1324, “Deviation/Waiver Request Process,” and determined that the driving factor for the deviation is still relevant and the risk associated with the deviation continues to be consistent with the agency’s risk tolerance level.
The assessor also verified that the implementation of compensating controls remains effective.</td></tr>
</table>

C.4 Examples: Assessment Findings of Provided at Agency Level

IA-5 – Authenticator Management		**Result: Provided at Agency Level**
Assessment Method(s): Examine		
Objective ID	IA-5.1.1	Provided at agency Level
Determine if the organization defines the time period (by authenticator type) for changing/refreshing authenticators.		Assessor Notes: This requirement is defined at the agency level. Per CSO-STD-0020, “Organization-Defined Values for System Security and Privacy Controls,” the organization defines the time period in which system authenticators for users and devices are changed/refreshed as: • at least every 5 years for Personal Identity Verification (PIV) cards and other hard tokens • at least every 3 years for PIV Authentication Certificate • at least every 3 years for soft digital certificates In accordance with CSO-STD-0001 “NRC Strong Password Standard” for passwords

IR-6(1) – Incident Reporting | Automated Reporting		**Result: Provided at Agency Level**
Assessment Method(s): Examine, Interview		
Objective ID	IR-6(1).1.1	Provided at agency Level
Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.		Assessor Notes: The assessor Interviewed the system ISSO, who stated that this requirement is provided at the agency level. Per CSO-STD-0021, “Common and Hybrid Security Control Standard,” IR-6(1) is a common control with responsibilities for the CSO. CSO CSIRT must use the US-CERT Incident Reporting System website as a secure automated mechanism for reporting computer security related incidents.

Example: Assessment Finding of Provided by <XYZ System>

MP-5 – Media Transport		**Result: Provided by <XYZ System>**
Assessment Method(s): Examine, Interview		
Objective ID	MP-5.1.3	Provided by <XYZ System>
Determine if the organization maintains accountability for system media during transport outside of controlled areas.		Assessor Notes: The assessor Interviewed the system ISSO, who stated that this requirement is provided by <XYZ System>. The assessor reviewed the service level agreement between <Organization 1> and <Organization 2> and confirmed that<ABC> relies on the <XYZ System> to protect and control digital media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. Hard copy media no longer needed are transported and disposed of in accordance with NRC policy.

C.5 Example: Assessment Finding of Not Applicable

SA-6 – Software Usage Restrictions		**Result: Not Applicable**
Assessment Method(s): Examine, Interview		
Objective ID	SA-6.1.3	Not Applicable
Determine if the organization controls and documents the use of peer to peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		Assessor Notes: The assessor interviewed the system ISSO, who stated that this requirement is not applicable. <ABC> does not use peer to peer software. Therefore, this requirement does not apply.

APPENDIX D ACRONYMS

AC	Access Control (control family)
ADAMS	Agencywide Documents Access & Management System
API	Application Program Interface
ARP	Address Resolution Protocol
AT	Awareness and Training (control family)
AU	Audit and Accountability (control family)
BIA	Business impact analysis
CA	Security Assessment and Authorization (control family)
CIO	Chief Information Officer
CIS	Center for Internet Security
CM	Configuration Management (control family)
CONOPS	Concept of Operations
CP	Contingency Planning (control family)
CPE	Common Platform Enumeration
CSO	Computer Security Office
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DAA	Designated Approving Authority
DISA	Defense Information Security Agency
DR	Deviation Request
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FOIA	Freedom of Information Act
FTS	Findings Tracking Sheet
GUI	Graphical User Interface

HVAC	Heating, Ventilation, and Air Conditioning
IA	Identification and Authorization (control family)
IIS	Internet Information Services
IP	Internet Protocol
IR	Incident Response (control family)
IRSD	Information & Records Services Division
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISDN	Integrated Services Digital Network
ISSO	Information System Security Officers
MA	Maintenance (control family)
MOU	Memoranda of understanding
MP	Media Protection (control family)
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OAR	Official Agency Record
OIS	Office of Information Services
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PDF	Portable Document Format
PE	Physical and Environmental Protection (control family)
PIA	Privacy impact assessment
PL	Planning (control family)
POA&M	Plan of Action and Milestones
PS	Personnel Security (control family)

PSTN	Public Switched Telephone Network
PTA	Privacy threshold analysis
RA	Risk Assessment (control family)
RMF	Risk Management Framework
RTU	Remote telemetry unit
SA	System and Services Acquisition (control family)
SAD	System architecture document
SC	System and Communications Protection (control family)
SCA	System Cybersecurity Assessment
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SI	System and Information Integrity (control family)
SIA	Security Impact Assessment
SITSO	Senior IT Security Officer
SLA	Service level agreement
SQL	Structured Query Language
SSP	System Security Plan
STIG	Security Technical Implementation Guide
VAR	Vulnerability Assessment Report
VPN	Virtual Private Network
VTC	Video Teleconferencing