Nuclear Regulatory Commission
Computer Security Office
Computer Security Process

Office Instruction:	CSO-PROS-1323
Office Instruction Title:	Information Security Continuous Monitoring Process
Revision Number:	2.0
Effective Date:	April 15, 2015
Primary Contacts:	Kathy Lyons-Burke, SITSO
Responsible Organization:	CSO/PCT
Summary of Changes:	CSO-PROS-1323, "Information Security Continuous Monitoring Process" defines the process that must be followed to perform continuous monitoring on systems owned and used by NRC.
Training:	As needed
ADAMS Accession No.:	ML14091A703

Concurrences			
Primary Office Owner	Policy, Standards, and Training		
Responsible SITSO	Kathy Lyons-Burke		**Date of Concurrence**
Directors	CSO	Tom Rich	04-Nov-14
	PCT	Kathy Lyons-Burke	04-Nov-14
	CSA	Thorne Graham	04-Nov-14

Concurrence Meeting Conducted on 04-Nov-14			
Attendees:	Tom Rich	Kathy Lyons-Burke	Thorne Graham

Table of Contents

Computer Security Process
CSO-PROS-1323

Information Security Continuous Monitoring Process

---

1 PURPOSE

CSO-PROS-1323, "Continuous Monitoring Process," provides the process that must be followed to maintain ongoing awareness of information security, vulnerabilities, and threats in support of United States Nuclear Regulatory Commission (NRC) risk management decisions for systems storing or processing NRC information up to, and including, the Safeguards Information (SGI) level. CSO-PROS-1323 defines the process that must be followed to perform information security continuous monitoring (ISCM) on systems owned and used by NRC.

An effective risk management program and related ISCM activities, support the shift from a static snapshot of the organization and system security posture to a near real-time, dynamic security status and is implemented at the agency and system levels. At the agency level, ISCM direction and compliance reviews are established to ensure System Owners are effectively conducting ISCM for their systems. At the system level, the System Owner implements an ISCM plan that addresses existing requirements to monitor changes to his or her systems and security controls to ensure the systems' security posture is not degraded.

ISCM activities are part of the mandatory information security management framework defined by the Federal Information Security Management Act (FISMA) and the security authorization process required by Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources. The ultimate objective of ISCM is the constant, near real-time detection and management of risk.

This document serves to assist System Owners and Information System Security Officers (ISSOs) in effectively conducting office and system level ISCM activities in support of agency-wide continuous monitoring, as well as assisting the Computer Security Office (CSO) in implementing the NRC Cybersecurity Program as defined in Management Directive and Handbook 12.5, NRC Cyber Security Program. The direction in this document applies to all systems operated and maintained by or on behalf of NRC, including other agency systems that NRC uses.

2 GENERAL REQUIREMENTS

An effective ISCM program is essential to support NRC risk management and is a critical component of the NRC's risk management program. In accordance with OMB Memorandum M-14-03, the ISCM program should:

- Provide a clear understanding of agency risk and help officials set priorities and manage such risk consistently throughout the agency; and

- Address how the agency will conduct ongoing authorizations of information systems and the environments in which those systems operate, including the agency's use of common controls.

Information obtained through ISCM provides NRC with risk information that is critical for risk management decisions regarding system changes, system authorizations, budget priorities, and activity priorities. ISCM information should be specific, actionable, timely, and available to decision makers on demand.

Continuous monitoring activities must be performed at the frequencies identified in "Minimum Required Frequencies for Continuous Monitoring Activities Defined in CSO-PROS-1323."

2.1 References

- CSO Web Page (http://www.internal.nrc.gov/CSO/) for policies, standards, processes, procedures, templates and guidance other than those specifically listed
- CSO-PROC-2104, "System Artifact Examination Procedure"
- CSO-PROS-1321, "System Cybersecurity Coordination Process for New Systems and System Changes"
- CSO-PROS-1323, "Continuous Monitoring Process"
- CSO-PROS-1324, "U.S. Nuclear Regulatory Commission Deviation Request Process"
- CSO-PROS-1325, "Authority to Use 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 Controls"
- CSO-STD-2030, "System Authorization Process"
- CSO-STD-6001, "System Change Significance Standard"
- CSO-TEMP-0001, "System Information System Security Officer (ISSO) Appointment Memo Template"
- CSO-TEMP-0002, "Office Information System Security Officer (ISSO) Appointment Letter"
- CSO-TEMP-1325, "Authority to Use Request Memo"
- CSO-TEMP-1511, "Proposed System Change Information Template"
- CSO-TEMP-2024, "Contingency Test Report Template"
- Federal Information Processing Standard (FIPS) 199, 140-2, "Security Requirements for Cryptographic Modules
- Federal Information Processing Standards and National Institute of Standards and Technology (NIST) publications can be found at: http://csrc.nist.gov/.
- Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347
- FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems"

- Minimum Required Frequencies for Continuous Monitoring Activities Defined in CSO-PROS-1323
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) 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 800-50, "Building an Information Technology Security Awareness and Training Program"
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-60, "Volume I, Guide for Mapping Types of Information and Information Systems to Security Categories"
- NIST Special Publication (SP) 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model"
- NRC Management Directive 12.5, NRC Cyber Security Program
- OMB Circular A-130, Management of Federal Information Resources
- OMB Memorandum M-14-03, Memorandum for the Heads of Executive Departments and Agencies: Enhancing the Security of Federal Information and Information Systems

2.2 Roles and Responsibilities

Table 1 provides the high-level roles and responsibilities associated with ISCM, as customized for NRC from NIST SP 800-137.

Table 1: Information Security Continuous Monitoring Roles and Responsibilities

Role	Role Responsibilities
Head of Agency: the Executive Director for Operations (EDO) has been delegated the authority to appoint.	Appoints the NRC Designated Approving Authority (DAA).
Risk Executive (Function): An Information Technology (IT) risk executive (assigned to the CISO) ensures that managing IT system-related security risks: (a) is consistent across the agency; (b) reflects the agency's risk tolerance; and (c) performs as part of an agencywide process that considers other agency risks affecting mission/business success.	Oversees NRC's ISCM strategy and program; reviews status reports from the ISCM process as input to information security risk posture and risk tolerance decisions and provides input to mission/business process and information systems tier entities on ISCM strategy and requirements; promotes collaboration and cooperation among NRC entities; facilitates sharing of security-related information; provides an NRC-wide forum to consider all sources of risk; and ensures that risk information is considered for continuous monitoring decisions.
Chief Information Officer (CIO): Delegates the authority to ensure compliance with the requirements imposed on the agency by FISMA and related policies, procedures, standards,	Leads the NRC's ISCM program; ensures that an effective ISCM program is established and implemented for NRC by: establishing expectations and requirements; working closely with authorizing officials and other stakeholders to provide funding, personnel, and other resources; maintaining working

Table 1: Information Security Continuous Monitoring Roles and Responsibilities

Role	Role Responsibilities
and guidelines. Ensures that the CIO, in coordination with other senior executives, reports annually on the effectiveness of the agencywide Cyber Security Program, including progress of remedial actions.	group relationships among NRC entities; and achieving program communication goals.
Chief Information Security Officer (CISO): Responsible for the NRC Cybersecurity Program	Establishes, implements, and maintains NRC's ISCM program; develops NRC ISCM program guidance (i.e., policies/procedures) for continuous monitoring of the security program and information systems; develops configuration management guidance for NRC; consolidates and analyzes Plan of Action and Milestones (POA&Ms) to determine NRC security weaknesses and deficiencies; acquires or develops and maintains automated tools to support ISCM and ongoing authorizations; provides training on NRC's ISCM program and process; and provides support to information owners/information system owners and common control providers on how to implement ISCM for their information systems.
Designated Approving Authority (DAA): The DAA is a committee appointed by the EDO consisting of authorizing officials with designated authority to assume formal responsibility for approving the operation of an IT system at an acceptable level of risk based on an agreed-upon set of implemented security controls. The DAA consists of senior executives with a level of authority commensurate with understanding and accepting such IT system-related security risks.	Assumes responsibility for ensuring NRC's ISCM program is applied with respect to a given information system; ensures the security posture of the information system is maintained; reviews security status reports and critical security documents to determine if the risk to NRC from operation of the information system remains acceptable; and determines whether significant information system changes require reauthorization actions and reauthorizes the information system when required.
Business Area Leader: A business area leader is an office director, a regional administrator, or a deputy executive director responsible for an NRC business area, such as nuclear reactor regulation.	Analyzes potential security impact to organization and mission/business process functions resulting from changes to information systems and their environments of operation; take steps to respond to risk as needed (e.g., request new or revised metrics, additional or revised assessments, modifications to existing common or Program Management (PM) security controls, or additional controls) based on the results of ongoing monitoring activities and assessment of risk; reviews monitoring results to determine if organizational plans and polices should be adjusted or updated; reviews monitoring results to identify new information on vulnerabilities; and reviews information on new or emerging threats as evidenced by threat activities present in monitoring results, threat modeling (asset- and attack-based), classified and unclassified threat briefs, United States Computer Emergency Readiness Team (USCERT) reports, and other information available through trusted sources, interagency sharing, and external government sources.
System Owner (SO): A system owner is an office director, regional administrator, or Office of Information Services (OIS)	Establishes processes and procedures in support of system-level implementation of NRC's ISCM program, including developing and documenting an ISCM strategy for the

Table 1: Information Security Continuous Monitoring Roles and Responsibilities

Role	Role Responsibilities
division director that has overall responsibility for the security of NRC systems owned by his or her organization or operated on behalf of his or her organization by another agency or by a contractor.	information system; participates in NRC's configuration management process; appoints a primary and alternate system ISSO; establishes and maintains an inventory of components associated with the information system; conducts security impact analyses on changes to the information system; conducting, or ensuring conduct of, assessment of security controls according to the ISCM strategy; prepares and submits security status reports in accordance with NRC policy and procedures; conducts remediation activities as necessary to maintain system authorization; revising the system-level security control monitoring process as required; reviews ISCM reports from common control providers to verify that the common controls continue to provide adequate protection for the information system; and updates critical security documents based on the results of ISCM.
Information Owner: An information owner provides requirements to IT system owners regarding the security controls for the IT systems where the information resides.	Establishes the potential impact of compromise of the confidentiality, integrity, and availability of their information and ensures that systems processing their information employ the necessary security controls to protect the information to an acceptable level of risk. The information significance, potential impact of compromise, and required security controls are identified by the information owner, and the information owner determines who can access the information, who can modify and delete the information, and how the information may be used.
Common/Hybrid Control Provider: A common/hybrid control provider is responsible for the security of a specific set of common/hybrid security controls used to protect multiple IT systems. The common/hybrid control provider is accountable for the security risk associated with operating his or her common controls.	Establishes processes and procedures in support of ongoing monitoring of common/hybrid controls; develops and documents an ISCM strategy for assigned common/hybrid controls; participates in NRC's configuration management process; establishes and maintains an inventory of components associated with the common/hybrid controls; analyzes changes that affect the common/hybrid controls to determine cybersecurity impact; ensures security controls are assessed according to the ISCM strategy; prepares and submits security status reports in accordance with NRC policy/procedures; conducts remediation activities as necessary to maintain common control authorization; updates/revises the common security control monitoring process as required; updates critical security documents as changes occur; and distributes critical security documents to individual information owners/information system owners, and other senior leaders in accordance with NRC policy/procedures.
Information System Security Officer (ISSO) – System: The designated security representative of an IT system owner. This is a trusted position with special access to and authority over an IT system. This role must not be assigned to an individual who has other trusted responsibilities (e.g., a system administrator should not be assigned	Supports NRC's ISCM program by assisting the system owner in completing ISCM responsibilities and by participating in the configuration management process.

Table 1: Information Security Continuous Monitoring Roles and Responsibilities

Role	Role Responsibilities
ISSO responsibilities).	
Information System Security Officer (ISSO) – Office: Serves as the ISSO representative and single point of contact for ISSO responsibilities for one or more offices or regions and communicates ISSO relevant information to the rest of the office's system-level ISSOs and computer professionals.	Supports NRC's ISCM program by conveying ISCM related information to all system ISSOs in the office or region and helping to resolve system ISSO issues.
Security Control Assessor: Determines if security controls are in place, operating as intended, and having the desired impact.	Provides input into the types of security-related information gathered as part of ISCM; assesses information system or program management security controls for NRC's ISCM program; develops a security assessment plan for each security control; submits the security assessment plan for approval prior to conducting assessments; conducts assessments of security controls as defined in the security assessment plan; updates the security assessment report as changes occur during ISCM; and updates/revises the security assessment plan as needed.
Policy Compliance and Training (PCT) Senior Information Technology Security Officer (SITSO)	Develops and distributes NRC's ISCM strategy; provides oversight of ISCM implementation; provides processes and procedures to support ISCM implementation.
Cyber Situational Awareness and Incident Response (CSAAR) SITSO	Supports ISCM Continuous Diagnostics and Mitigation (CDM) implementation by NRC

3 ISCM STRATEGY

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* describes an agency-wide approach to continuous monitoring that supports risk-related decision making at the:

- NRC level (Tier 1)
- Mission/business processes level (Tier 2)
- Information systems level (Tier 3)

3.1 NRC Level: Tier 1

Tier 1 ISCM activities relate to agency-wide information security governance that addresses agency-wide risk, including core mission and business functions. ISCM at this level is defined by the NRC risk management strategy that defines how NRC assesses, monitors, and mitigates risk, including agency oversight to ensure the strategy is effective.

Tier 1 officials are the NRC DAAs, including the Major Information Technology (IT) Investments DAA and the Non-Major IT Investments DAA. Each NRC DAA is a committee of individuals appointed by the NRC Executive Director for Operations (EDO). The DAAs make risk management decisions based on:

- Security-related information provided on the Cybersecurity Risk Dashboard (CRDB);

- Information presented by the CSO during briefings;
- Information submitted as part of authorization packages;
- Information submitted within formal requests for deviations and waivers;
- Information documented in Office of Inspector General Audits;
- Information documented in Financial Audits;
- Information documented in penetration test reports; and
- Information obtained from other risk-based data sources.

More information on the NRC DAA can be found at: http://www.internal.nrc.gov/CSO/DAA.html

Tier 1 metrics directly support agency-wide information security governance risk management decisions. Tier 1 metrics are provided to the Tier 1 officials during DAA risk briefings and via the NRC Cybersecurity Risk Dashboard (CRDB).

3.2 Mission/Business Processes Level: Tier 2

Tier 2 ISCM activities relate to information security activities that impact one or more mission or business processes. Officials with responsibility for those mission or business processes must oversee the associated risk management activities for those processes. Tier 2 includes the NRC Cybersecurity Program as well.

Tier 2 officials are the Business Area Leaders (Business Line Managers) and the Chief Information Security Officer, who must determine the level of risk tolerance with respect to their business areas and the Cybersecurity Program respectively.

Tier 2 metrics identify issues that impact mission or business processes. Tier 2 metrics are provided to the Tier 2 officials via Business Area Risk Assessments (BARAs) and the CRDB.

3.3 Information Systems Level: Tier 3

Tier 3 ISCM activities relate to information systems operated by or on behalf of NRC. System owners and common and hybrid control providers must ensure in a continuous manner that security controls are in place, operating as intended, and having the desired effect. In addition, cybersecurity status, such as security alerts, incidents, and threats are included in Tier 3. System security assessments support system change decisions, system authorization decisions, and ISCM.

Tier 3 officials are system owners, information owners, and common/hybrid control providers.

Tier 3 metrics identify issues with systems. Tier 3 metrics are provided to the Tier 3 officials via Chief Information Security Officer (CISO)-tier 3 official meetings, BARAs, and the CRDB.

Activities and metrics from the Tier 3 level support risk decisions made at the Tier 1 and Tier 2 level.

Each information owner must specify the potential impact of compromise of the confidentiality, integrity, and availability of their information and ensure that systems processing their information employ the necessary security controls to protect the information to an acceptable level of risk. For example, information about employees, such as social security number, home

address, etc. would be owned by the Chief Human Capital Officer, and information related to employees' clearances would be owned by the Director, Office of Administration. The information significance, potential impact of compromise, and required security controls are identified by the information owner, and the information owner determines who can access the information, who can modify and delete the information, and how the information may be used.

Each system owner and common/hybrid control provider, in coordination with information owners, must develop and maintain a strategy for continuous monitoring of system controls to maintain an understanding of cybersecurity control effectiveness and status. The plan is initially developed during the system design or upon decision to procure a commercial product and is updated to reflect system changes, changes to the environment, and changes in threats. The plan must meet agency-wide reporting requirements at a minimum and include:

- Configuration management controls and processes;
- Security analyses of proposed system changes;
- Security control assessments that determine if the security controls are in place, operating as intended, and having the desired impact; and
- Security status reporting.

The plan must address the following:

- How the system-level ISCM strategy supports risk management at all 3 tier levels, including system and agency architecture and operational environment;
- How security controls, including system-specific, common, and hybrid security controls, are monitored for effectiveness (assessments) and security status;
- How and with what frequency are security control assessment findings reported; and
- How the system-level ISCM strategy minimizes compromises to the security architecture and prevents or minimizes impact on business and mission functions.

System owners determine assessment frequencies of security controls based on drivers from all three tiers, however, they must meet the minimum NRC required frequency.

3.4 System Authorizations

The operational environment is the environment in which mission functions are performed. All tools installed or used within the operational environment must be authorized by the DAA. This includes all systems operated by or on behalf of NRC. System owners are encouraged to identify and obtain approval for tools in advance of planned use so that the time required for the authorization does not delay planned activities.

System owners must obtain a cybersecurity Authority to Operate (ATO) before placing a system into the operational environment or using that system in any way for NRC purposes. The operational environment includes any use of real data, regardless of the connectivity. All NRC IT resources must belong to an NRC IT system, and must therefore be part of a system ATO before being placed into operation. This includes all new systems and modifications to existing systems. To maintain a system authorization, the system owner must ensure that the system adheres to any specified ATO conditions and the system owner must maintain system continuous monitoring. The NRC system authorization process is defined in CSO-STD-2030,

"System Authorization Process." Authorization of other agency systems that NRC uses are performed in accordance with CSO-PROS-1325, "Authority to Use Process."

At any point in time, the DAA can require that a system/subsystem undergo a re-authorization process. This requirement is typically based upon the risk associated with a system either due to a changing threat environment, a system compromise, or a lack of sufficient continuous monitoring.

3.4.1 Periodic Authorizations

A periodic authorization is an authority to operate for a specific time period. Historically, all systems/subsystems received an authority to operate for 3 years. A system/subsystem re-authorization is required prior to the periodic authorization expiration, unless the system is decommissioned prior to the expiration date.

3.4.2 Ongoing Authorizations

An ongoing authorization is an authority to operate granted for an indefinite period of time. An ongoing authorization is granted at the completion of a full authorization process.

Continuous monitoring is even more critical for systems in an ongoing authorization state since there isn't a fixed period of time when all controls will be fully assessed again. This state depends upon an ongoing assessment of the security controls to determine if they are in place, operating as intended, and having the desired effect. Continuous monitoring supports the current reality of constantly changing environments, threats, and technologies, and ensures that new threat or vulnerability information is evaluated as it becomes available. This evaluation then drives adjustments to security requirements or individual controls as needed to maintain authorization decisions.

3.4.3 Change Authorization

All changes except minor changes must have a change authorization prior to deploying in an operational environment. See Section 5.13.

3.4.4 Standalone Laptop, Tablet, and Personal Computer Authorization

All NRC standalone laptops, tablets, and personal computers must belong to a system, and that system must be authorized to operate. Each office and region can have 3 types of laptop/tablet/standalone personal computer systems: classified, Safeguards Information (SGI), and general. The office's classified laptop/tablet/standalone personal computer system boundary includes all laptops, tablets, and standalone personal computers that process classified information. The office's SGI laptop/tablet/standalone personal computer system boundary includes all laptops, tablets, and standalone personal computers that process SGI, but not classified information. The office's general laptop/tablet/standalone personal computer system boundary includes all laptops, tablets, and standalone personal computers that process information that is not classified information and not SGI.

System owners must submit information to obtain an authority to operate each of their laptop/tablet/standalone personal computer systems using the processes, standards, and templates appropriate to the system. These can be found on the CSO web page.

Note that System Owners are encouraged, to the extent practical and based upon business needs, to use seat-managed laptop/tablet/standalone personal computers distributed by OIS

instead of maintaining their own. OIS is the System Owner for the seat-managed laptops/tablets/standalone personal computers and will ensure the above requirements are satisfied.

3.5 Automation

Automated solutions are desirable to reduce the cost and effort required to perform activities, resulting in more frequent data and an ability to adjust security controls based upon new threats and vulnerabilities. Automated solutions usually apply to situations where the required activity is well defined and requires little human intervention. Many ISCM tasks require human interaction and cannot be automated.

Automation should be applied where:

- Information is obtained from a variety of electronic sources;
- Activities use open specifications such as the Security Content Automation Protocol (SCAP);
- Tools integrate with other cybersecurity relevant tools;
- Tools are cost-effective;
- Tools aid in meeting NRC and federal requirements;
- Tools enable tailored reporting; and
- Tools consolidate data into formats used by other cybersecurity relevant tools.

Tools used to support cybersecurity risk assessment must be constantly evaluated to ensure the tools are assessing the risk based upon NRC requirements.

4 CYBERSECURITY AWARENESS AND TRAINING

OMB Circular A-130, Management of Federal Information Resources, and FISMA require agencies to ensure all individuals receive security awareness training and specialized training focused on their cybersecurity role and responsibilities. All office directors and regional administrators must ensure that all staff and contractors complete the annual computer security awareness course by the required date.

Office directors and regional administrators must ensure that staff that are persuaded to perform inappropriate actions by emails sent as part of agency-wide phishing awareness exercises take anti-phishing courses provided in iLearn and that repeat offenders receive additional counseling and any agency-stipulated consequences.

4.1 Cybersecurity Role Identification

The Federal Information Security Management Act (FISMA) requires that all personnel with significant cybersecurity responsibilities be appropriately identified. Effective June 14, 2004, the Office of Personnel Management (OPM) required agencies to identify employees with significant cybersecurity responsibilities and develop a cybersecurity training plan. The plan must include provisions for role-specific training as detailed by the National Institute of Standards and Technology (NIST) guidance (Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" and SP 800-50, "Building an Information Technology Security Awareness and Training Program"). The Nuclear Regulatory

Commission (NRC) cybersecurity training plan is located at: http://www.internal.nrc.gov/CSO/training.html#Role-based. The current training plan will be transitioning to the Cybersecurity Workforce Development Plan in the near future.

Office directors and regional administrators must maintain at the NRC required frequency the list of individuals in their office or region who are assigned significant cybersecurity roles. All division directors and above are executives and must take role-based training for executives. The NRC significant cybersecurity role definitions are available at: http://www.internal.nrc.gov/CSO/Cybersecurity-Roles.html. The current list of assigned significant cybersecurity roles can be found at: http://www.internal.nrc.gov/CSO/training.html.

4.1.1 System ISSOs

Appointment of Primary and alternate system ISSO must be provided by a memo from the system owner to the CISO using CSO-TEMP-0001, "System Information System Security Officer (ISSO) Appointment Memo Template". Notification of assignment or de-assignment of an individual to a significant cybersecurity role other than the ISSO must be provided in writing to the CISO. A list of courses available in iLearn to assist with role-based training requirements can be found at: http://www.internal.nrc.gov/CSO/documents/CyberSecurityTrainingTable.pdf

4.1.2 Office ISSOs

System owners must appoint an office ISSO to represent the office and all ISSOs within the office to the ISSO forum and to CSO. The system owner must appoint the primary and alternate office ISSO using a memo issued to the CISO in accordance with CSO-TEMP-0002, "Office Information System Security Officer (ISSO) Appointment Letter". The memo must be an Official Agency Record (OAR) and the accession number provided via an email to the RidsCsoMailCenter Resource email box. Additional information about the ISSO forum can be found at: http://www.internal.nrc.gov/CSO/ISSOForum.html

Offices may decide to have a single individual represent multiple offices. If this is the case, the appointment memo should so indicate. System owners must ensure that the primary or alternate office ISSO participates in ISSO forum meetings. ISSO forum meetings provide the mechanism to distribute information to the NRC ISSO community and to enable ISSOs to share issues/concerns with CSO and with each other.

4.2 Cybersecurity Role-Based Training

Office directors and regional administrators must ensure that personnel assigned to cybersecurity roles complete required role-based training, as identified in the workforce development plan, by the required date (see role-based training table). The training requirements for each individual with a role can be found at: http://fusion.nrc.gov/cso/team/FCO/Cyber%20Risk%20Dashboard/Pilot/DataFiles/Role-based%20Training/Role-Based%20Cybersecurity%20Training%20Requirements.xls

CSO provides system administrator (applicable to system/network/database administrator roles) and ISSO courses for one year of the three year training cycle. The training for the other two years must be obtained from commercial sources (e.g., iLearn/Skillsoft, Global Knowledge, SANS Institute, Learning Tree, ISC^2).

5 CONTINUOUS MONITORING OF NRC ESTABLISHED SYSTEMS

NRC established systems are systems created or modified by or on behalf of NRC for NRC mission needs. Office directors and regional administrators must engage the CSO at the start of any initiative to develop a new IT system or to modernize or enhance an existing system. System security is a critical function and should be addressed at the onset of any IT project. This includes systems operated on behalf of NRC. System owners and common and hybrid control providers must ensure in an on-going continuous manner that security controls are in place, operating as intended, and having the desired effect.

At the system level, continuous monitoring involves five key tasks: (1) assessing security control effectiveness, (2) addressing risks identified during assessments (including vulnerability scans and configuration checks of system components), (3) maintaining system security documentation, (4) performing required tests, and (5) reporting the security state of the system to designated organization officials. The security-related information obtained and reported during continuous monitoring informs NRC DAA risk-based decision making.

Continuous monitoring tasks are performed concurrently. For example, system personnel respond to risks that were identified during periodic vulnerability scans, maintain information within the system Plan of Action and Milestones (POA&M), and maintain system documentation on an ongoing basis. Internal and independent assessments of the implementation of security controls are also conducted throughout the cycle.

The output of one task typically drives the activities required during other tasks. For example, if on review of a system authorization package, the DAA issues conditions for the authorized operation of a system:

- the system ISSO must respond to the conditions and
- an independent assessor must determine whether or not the DAA conditions were adequately addressed.

Each of these activities necessitates an update to impacted system security documentation to ensure that the security state of the system at the time is captured and accurately reported.

All systems must meet NRC cybersecurity policy and standards, including configuration standards. This also applies to laptops and standalone computers. Cybersecurity standards requirements can be found on CSO's Cybersecurity Standards website at http://www.internal.nrc.gov/CSO/standards.html. If a CSO specific standard does not exist, the system must be configured in accordance with Defense Information Systems Agency (DISA) standards, checklists, and guidance. In the absence of both CSO standards and DISA requirements, the Center for Internet Security (CIS) benchmarks must be used. In the absence of CSO standards, DISA requirements, and the Center for Internet Security (CIS) benchmarks, industry and vendor best practices must be used. Any implementation differences from these standards require DAA authorization via the deviation/waiver process (CSO-PROS-1324).

The frequency of Periodic System Cybersecurity Assessment s (PSCAs) is not static (uniform across all NRC systems); the CSO ISCM program has established frequencies that support the periodic assessment of security controls based on the system's authorization state and the NRC's determination of the following:

- The volatility of each control (the likelihood of the control changing over time subsequent to its implementation),
- The criticality of the function supported by each security control. For example, the controls implemented to protect vital security functions (e.g., firewalls or log management servers) should be assessed frequently as they provide a critical security function to the overall system.

5.1 System Security Control Types

There are 4 types of system security controls and each type is described below:

- Core security controls
- Common security controls
- System-specific security controls
- Hybrid security controls

5.1.1 Core Security Controls

Controls determined to be volatile, to support critical system functions (including security functions), or are identified as being critical based upon current situational awareness are considered the NRC core controls. Each year, CSO reviews system and organization level security-related information (e.g., the information reported concerning system security control assessments and risk assessments), the output of NRC ISCM strategy reviews, and threat and vulnerability patterns identified during the previous year. Each security control is then evaluated within the context of this information, and the ISCM program determines whether or not an assessment of the control should be required during the coming year. Finally, the ISCM program publishes and disseminates the list of core controls, and posts them to the CSO Web Page at: http://www.internal.nrc.gov/CSO/System_Authorization.html.

External reporting requirements also influence the selection of core controls. For example, if the OMB requires the NRC to report key security metrics at a specific frequency, associated security controls would be monitored and assessed at the frequency required to support the OMB reporting requirement.

All core security controls must be independently assessed at least annually.

5.1.2 Common Security Controls

Common security controls are security controls that are inherited by one or more systems. Common security control providers, as the system owner, are accountable for the security risk associated with operating his/her common security controls. Because these controls protect multiple systems of differing sensitivity levels, common controls must be implemented with regard to the highest sensitivity level among the inheriting systems.

Common control providers, as the system owners for the systems providing the controls, are accountable for the security risk associated with operating his/her common controls. However, issues with implementation of common controls are often detected when assessing the control for the inheriting system. Therefore, the system ISSO must ensure that the implementation of each common security control is independently assessed at the NRC required frequency to determine whether the control is effective.

If the Independent Assessment Team (IAT) determines that the implementation of the common control is not providing the intended protection for the inheriting system, the overall implementation status of the control must be assessed as "provided by <ABC>", where <ABC> represents the providing system's acronym, and notes must be provided indicating that the control is not providing the intended protection.

All common security controls must be independently assessed at least triennially, with at least one-third of the controls assessed annually.

Therefore, the system ISSO must ensure that:

- The controls established to support critical system functions (e.g., those functions deemed to be critical in a system's Business Impact Analysis) are assessed frequently.
- The implementation of each common security control is independently assessed at the NRC required frequency.

5.1.3 System-Specific Security Controls

System specific security controls are controls that are implemented for a system that have not been designated by the NRC as a common control, and are not provided by another system as an inherited control. For hybrid controls, one portion of the control is system specific (implemented for the system itself), and another portion of the control is either provided by a common control provider or is inherited from a different system.

All system-specific security controls must be independently assessed at least triennially, with at least one-third of the controls assessed annually.

System-specific control providers, as the system owner, are accountable for the security risk associated with operating his/her system-specific controls (or, in the case of hybrid controls, the system-specific portion of the controls). Therefore, the system ISSO must ensure that:

- The controls established to support critical system functions (e.g., those functions deemed to be critical in a system's Business Impact Analysis) are assessed frequently.
- The implementation of each system specific security control is independently assessed at the NRC required frequency.

5.1.4 Hybrid Security Controls

A hybrid control is a security control that is implemented in a system in part as a common control or a control inherited from another system, and in part as a system-specific control.

Hybrid controls are provided by two control providers: the system owner of the system that provides the common or inherited portion of the control, and the system owner of the system specific portion of the control. Therefore, each provider is accountable for the security risk associated with operating the system with his/her portion of the control.

An example of how a control could be a hybrid control follows:

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

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

Control Description:

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

Provider Responsibilities:

OIS provides cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions (e.g., Citrix, VPN) for NRC systems connected to the NRC domain in accordance with NRC requirements.

System owners ensure that applications providing remote access methods through non-NRC controlled networks provide cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions in accordance with NRC requirements.

All hybrid security controls must be independently assessed at least triennially, with at least one-third of the controls assessed annually.

When assessing the effectiveness of the system specific portion of hybrid security controls, system ISSOs are not responsible for the effective implementation of the common or inherited portion of the control. However, the system ISSO must ensure that the implementation of the system specific portion of the security control is independently assessed at the NRC required frequency to determine whether the portion of the control they are responsible for is effective.

If, during the assessment of the implementation of the system specific portion of the control, the IAT determines that the portion provided by another system is not implemented properly, the overall implementation status of the control must be assessed as deficient, and notes must be provided describing the nature of the deficiency. The ISSO must report the deficiency to the ISSO and system owner of the providing organization so the deficiency can be remediated.

5.2 Monitoring Requirement Levels

Monitoring requirements differ based upon the sensitivity of the information, the operating environment, current threats, and known vulnerabilities: the higher the risk, the stronger the continuous monitoring requirements. Tier 1 officials determine the level of risk acceptance and frequency of risk evaluation using continuous monitoring methods.

In the same vein, monitoring frequencies vary between requirements and based upon current risk and threat assessments. For example, a system that contains information known to be a target of current threats, a system with many known vulnerabilities, and a system that was recently compromised may be required to perform more frequent and thorough continuous monitoring of cybersecurity controls, irrespective of the system categorization.

Required security controls also have many components, including enhancements. As a result, a single control may have different continuous monitoring requirements and frequencies associated with the different components.

Criteria used to determine continuous monitoring frequencies include, but are not limited to:

- Security control volatility (e.g., configuration settings require more frequent assessments)

- System categorizations/impact levels (e.g., in general, a high impact level requires more frequent assessments than a low impact level)
- Items (e.g., security controls, information) that provide critical functions (i.e., critical functions require more frequent assessments)
- Security controls with identified weaknesses (e.g., existing risks documented in security assessment reports (SARs))
- NRC risk tolerance
- Current threat information (e.g., organizations with a low tolerance for risk (e.g., organizations that process, store, or transmit large amounts of proprietary and/or personally identifiable information (PII), organizations with numerous high-impact systems, organizations facing specific persistent threats) monitor more frequently than organizations with a higher tolerance for risk (e.g., organizations with primarily low- and moderate-impact systems that process, store, or transmit very little PII and/or proprietary information))
- Vulnerability information (e.g., known vulnerabilities require more frequent continuous monitoring and if a specific product manufacturer provides software patches monthly, vulnerability scans are conducted on that product at least that often)
- Risk assessment results
- External reporting requirements (e.g., Department of Homeland Security (DHS), OMB)

5.3 Continuous Monitoring Reporting

The system owner must ensure that all required continuous monitoring reporting is accomplished via documents submitted using the Agencywide Documents Access and Management System (ADAMS) Accession Number (ML number) of OAR. "View Content" and "View Props" access rights must be extended to groups "CSO Contractor Group", "CSO Employees Group", and "OIG [Office of the Inspector General] -FISMA Audit" for all documents uploaded to ADAMS.

System owners must submit information to CSO by emailing the accession number to the RidsCsoMailCenter Resource email box.

Current information regarding the status of continuous monitoring requirements can be found on the CRDB.

System ISSOs are responsible for ensuring that all system-level security controls within the system's security control baseline are implemented correctly, operating as intended, producing the desired outcome with respect to meeting the security requirements for the system, and are effective over time.

Each system's security control baseline, along with a description of the implementation of each control and the rationale for tailoring controls is documented in a supporting System Security Plan (SSP). The baseline is established using:

- The CSO approved system security categorization/sensitivity level (established in accordance with Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems" and NIST SP

800-60, “Volume I, Guide for Mapping Types of Information and Information Systems to Security Categories”);

- The security control catalog provided in NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations;” and
- Additional controls implemented to provide additional protection to critical or high risk system assets or functions.

5.4 Configuration Management

Configuration Management (CM) involves the control of IT system components, features, and assurances defined as configuration items by monitoring changes to a system’s hardware, software, firmware, testing, and test fixtures throughout the life cycle of a system. System configuration management is directly related to system security posture and agency risk and is the responsibility of the system owner.

CM provides the following organizational benefits:

- Streamlining of configuration and change processes
- Reduction of costs through centralized record-keeping and change management
- Reliable agency-wide accounting of system states
- Current, accurate, and easily retrievable and auditable system documentation
- Assurance that systems remain configured to appropriate standards
- Assurance that system changes are properly evaluated for impact on security, functionality, and availability
- Assurance that system changes are appropriately authorized
- Prevention and detection of changes that could detrimentally affect the security posture of NRC systems.

5.5 Configuration Monitoring

The system ISSO must monitor the system to ensure the system (all components of the system) is configured in accordance with NRC configuration requirements and to ensure the components are consistent with the system component inventory that was authorized by the DAA. The system ISSO must have monitoring processes and procedures that identify unauthorized changes to the system configuration and must correct those unauthorized changes immediately. In addition, the system ISSO must determine why the unauthorized changes were made and must take action to ensure unauthorized changes are not made in the future. Formal configuration scan reports are required to be submitted to CSO at the NRC required frequency, however, the ISSO is responsible for maintaining the required configuration and should monitor as frequently as necessary to ensure the settings are maintained.

Components that are not configured per the NRC approved standards are vulnerable to known exploits associated with specific configuration settings. System ISSOs must verify that configuration settings comply with NRC approved secure baseline configurations, using NRC provided SCAP validated scanning tools and CSO validated configuration templates when available.

Unauthorized configuration changes are reportable cybersecurity incidents and must be reported to the Computer Security Incident Response Team (CSIRT).

A history of regular configuration checks (and the secure configuration of system components) demonstrates that an organization is proactive in maintaining the security state of its systems on an ongoing basis.

5.6 Vulnerability Monitoring

System vulnerabilities can be exploited and result in a compromise to information confidentiality, integrity, or availability. As a result, vulnerability management is critical in maintaining the system security posture and an acceptable level of risk to the agency.

Many times software flaws or misconfigurations cause system vulnerabilities, so it is important that the system ISSO maintain an understanding of vulnerabilities and remediations that have been identified for software and hardware that are implemented as part of systems for which they are responsible. There are a variety of sources for the vulnerability and remediation information, including but not limited to information provided by the following:

- CSO
- United States Computer Emergency Readiness Team (US-CERT)
- Vendors
- Vulnerability analysis tools
- Independent audits and assessments
- Penetration tests

The system ISSO must monitor the system for known or suspected vulnerabilities. The system ISSO must have monitoring processes and procedures that identify those vulnerabilities and remediations and must perform remediations in accordance with CSO-STD-0020, "Organization Defined Values for System Security Controls".

Regular vulnerability scanning allows ISSOs to determine whether the security controls implemented to protect their systems from known exploits and threats continue to be effective. Automated scanning tools are available that seek out weaknesses (based on known security flaws), test system components and hosted applications to determine whether the flaws exist, and then generate reports of detected weaknesses that need to be remediated. Formal vulnerability scan reports are required to be submitted to CSO at the NRC required frequency, however, the ISSO is responsible for maintaining the required configuration and should monitor as frequently as necessary to ensure vulnerabilities are identified and mitigated appropriately.

System vulnerability remediation must be prioritized according to the significance of the vulnerability (e.g., how easily the vulnerability could be exploited), the criticality of the assets that could be exploited, and the potential impact of compromise of the information that could be compromised. Remediation actions must be performed in accordance with CSO-STD-0020.

Patching is the process of applying software designed to fix security issues and vulnerabilities and improve usability or performance. System Owners must patch, scan, check the security of their systems, and remediate findings with the rigor and frequency appropriate for the system sensitivity level. System patching, vulnerability scans, and finding remediation must be

performed in accordance with CSO-STD-0020 and CSO-PROS-1401, "Periodic System Scanning Process," and in accordance with continuous monitoring requirements.

A history of regular vulnerability scans (and the timely remediation of identified weaknesses) demonstrates that an organization is proactive in maintaining the security state of its systems on an ongoing basis.

If weaknesses are identified that the system owner believes should not be remediated due to an adverse impact to system operations, an adverse impact to organization business processes, or because the cost of remediation exceeds the risk posed by a potential security incident, the system owner must obtain DAA authorization via the deviation/waiver process (CSO-PROS-1324).

5.7 Contingency Plan (CP) Testing

CP testing validates recovery capabilities to improve CP plan effectiveness and overall organizational preparedness to execute the plan. This provides assurance that the plan remains current with system and organizational changes. CP test report dates must not exceed the required CP test frequency requirement from the date of the prior CP test report. To ensure OIS has resources available when needed where OIS coordination is required, the System Owner should schedule CP testing with OIS in advance of the test.

System ISSOs must ensure that their system's Contingency Plan is tested at a minimum per the values established for the CP-4 security control in CSO-STD-0020, "Organization Defined Values for System Security Controls." CSO-STD-0020 provides the required frequency, type of test (table-top, functional exercise, or actual test), and specific test requirements for systems with low, moderate, or high availability system sensitivity levels.

The following list identifies major milestones that must be incorporated into the system CP testing schedule:

1. Conduct and document a Business Impact Analysis (BIA) or update the existing BIA.
2. Develop a Contingency Test Plan for testing the CP.
3. Conduct annual CP training for staff with contingency planning roles and responsibilities.
4. Coordinate testing with affected organizations.
5. Execute CP testing according to the Contingency Test Plan.
6. Develop a Contingency Test Report to document the results of testing.
7. Ensure that weaknesses identified through CP Testing are incorporated into the system's POA&M in accordance with CSO-PROS-2016, "Plan of Action and Milestones Process."
8. Ensure that the CP test information is entered into relevant POA&M items in accordance with CSO-PROS-2016.
9. Update the CP to reflect the results of CP testing and lessons learned within the NRC required frequency of completion of testing and delivery of the CP Test Report.

System ISSOs must document contingency plan test results using CSO-TEMP-2024, "Contingency Test Report Template" (available at http://www.internal.nrc.gov/CSO/security_templates.html), update the contingency plan as required based upon the contingency test results, and record the contingency test results and updated contingency plan as official agency records in ADAMS. Notification of completion along with the ADAMS accession numbers must be provided via the RidsCsoMailCenter Resource.

5.8 Maintaining System Security Documentation

System ISSOs must routinely maintain the system security documentation that provide organization officials with the system security information needed to make informed recommendations and risk-based decisions concerning their systems. A history of consistent, ongoing maintenance of system policies and procedures, SSPs, POA&Ms, system inventory, configuration baselines, and contingency plans demonstrates that an organization is proactive in:

- Planning for the implementation of security controls,
- Planning for the remediation of identified findings,
- Assessing the risk posed to the organization (and NRC) by operating the system with the findings,
- Documenting the current as built state of the system in support of the implementation of appropriate security controls for the system and specific system components, and
- Planning for the recovery of essential missions and business functions during a contingency event.

All system security documentation must be developed and maintained in accordance with NRC-issued templates (available at http://www.internal.nrc.gov/CSO/security_templates.html). CSO-PROC-2104, "System Artifact Examination Procedure" provides the examination criteria to be applied to each documentation artifact to ensure completeness. All system security documentation must be maintained continuously and be current in accordance with NRC frequency requirements.

5.9 Independent System Cybersecurity Assessments

While the system ISSO monitors the system security state on a continuous basis, independent assessments are required to ensure the security controls are in place, operating as intended, and having the desired effect. The system owner is responsible for funding and employing an IAT to perform independent assessments for all system components.

5.9.1 Authorization System Cybersecurity Assessments

Authorization System Cybersecurity Assessments (ASCAs) are independent assessments conducted by an IAT in support of the NRC ISCM program. ASCAs are conducted in support of the system authorization process, security impact analyses, and as a regular method of ensuring system continuous monitoring activities are effective. An ASCA can be conducted on the entire system or a portion of the system depending on the reason for the ASCA. A full system authorization and re-authorization requires a full ASCA on the entire system. A subsystem or partial system authorization or re-authorization requires a full ASCA for the components being authorized. During a full ASCA, every security control in the identified

assessment boundary is assessed, and vulnerability scans and configuration checks are conducted of system components per NRC sampling requirements.

The security related information and metrics obtained during an ASCA are used by the NRC ISCM program to analyze assessment results throughout the agency. For example, assessment findings must be tracked within the system POA&M; the system POA&Ms are then used to analyze assessment findings across multiple systems and organizations, provide an analysis of reported findings to agency officials and the OMB, and refine the NRC ISCM program and strategy. System ISSOs must record the ASCA report as an official agency record in ADAMS. Notification of completion along with the ADAMS accession number must be provided to the CSO/Policy, Compliance, and Training (PCT) Senior IT Security Officer (SITSO).

ASCAs include core controls, system-specific security controls, hybrid security controls, and inherited controls.

System ISSOs must also ensure that full ASCAs are conducted whenever changes are proposed that could potentially impact the security state of the system/subsystem or the system/subsystem's environment of operation.

The IAT works with the System Owner to:

1. Develop an assessment schedule.

2. Develop and submit to CSO for review prior to test execution an assessment plan for the system.

3. Perform a comprehensive security assessment of the selected security controls using the assessment plan.

4. Document the results of the security controls testing in an ASCA report.

5. Ensure that weaknesses identified in the ASCA are incorporated into the system's POA&M in accordance with CSO-PROS-2016.

5.9.2 Periodic System Cybersecurity Assessments

Periodic System Cybersecurity Assessments (PSCAs) are independent assessments conducted by an IAT in support of the NRC ISCM program. PSCAs are conducted periodically in support of continuous monitoring. A PSCA can be conducted on the entire system or a portion of the system depending on the reason for the PSCA.

PSCAs include core controls, system-specific security controls, hybrid security controls, and inherited controls, however, PSCAs only involve a subset of the controls: The CSO identifies for each assessment period a set of core security controls that must be assessed. This requirement provides the necessary assurance that federally mandated and NRC defined security controls are being implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The security related information and metrics obtained during a PSCA are used by the NRC ISCM program to analyze assessment results throughout the agency. For example, assessment findings must be tracked within the system POA&M; the system POA&Ms are then

used to analyze assessment findings across multiple systems and organizations, provide an analysis of reported findings to agency officials and the OMB, and refine the NRC ISCM program and strategy. System ISSOs must record the PSCA report as an official agency record in ADAMS. Notification of completion along with the ADAMS accession number must be provided to the CSO/Policy, Compliance, and Training (PCT) Senior IT Security Officer (SITSO).

Testing completion dates must not exceed the required assessment frequency requirement from the date of the prior assessment report. The IAT works with the System Owner and system ISSO to:

1. Develop an assessment schedule.

2. Select controls that must be tested. These controls include CSO-defined core controls, controls associated with POA&M weaknesses that were closed within the past year, compensating controls and/or mitigating factors related to approved Deviation Requests (DRs), and any other additional controls selected by the DAA, CSO, or the System Owner.

3. Develop and submit to CSO for review prior to test execution an assessment plan for the system.

4. Perform a comprehensive security assessment of the selected security controls using the assessment plan.

5. Document the results of the security controls testing in an SCA report.

6. Ensure that weaknesses identified through SCAs are incorporated into the system's POA&M in accordance with CSO-PROS-2016.

7. Ensure that the SCA test completion information is entered into POA&M items that required completion of the SCA in accordance with CSO-PROS-2016.

5.10 POA&M Management

CSO-PROS-2016 prescribes the mechanism to identify, assess, prioritize, and monitor the progress of corrective actions pertaining to security weaknesses and provides agency direction for the management and tracking of corrective efforts relative to known weaknesses in Cybersecurity controls.

POA&Ms must be maintained at the NRC required frequency. In order to assist System Owners in effectively managing IT system risks, CSO periodically assesses POA&Ms from an agency risk perspective to facilitate security improvements throughout the agency.

5.11 Responding to Identified Weaknesses and Risks

System ISSOs must respond to any system cybersecurity findings that are identified by remediating the findings or by asking the DAA to accept the risk associated with the findings in formal, documented deviation/waiver requests. Remediation of findings may involve modifying or implementing additional security controls, applying security patches or upgrades, configuring system components per NRC approved configuration standards, or developing or updating system documentation deemed to be deficient. In rare instances and instances of system compromise, the system may be taken offline or decommissioned.

System ISSOs must ensure that legitimate critical, high, and moderate risk findings are remediated within the timeframes established for the RA-5 control in CSO-STD-0020, "Organization Defined Values for System Security Controls," and must track the status of each of finding within the system POA&M in accordance with CSO-PROS-2016. Low risk findings should be fixed as part of routine operations and maintenance activities.

5.11.1 Modify or Implement Additional Security Controls

If the implementation of a control was determined to be significant and deficient, system ISSOs must ensure that the control is remediated (or implemented) such that it is operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.

Remediation may involve, for example, implementing additional protection throughout the system using a technical solution (e.g., a firewall, an automated auditing mechanism, or an automated configuration management mechanism), revising and disseminating system policies and procedures, ensuring that organization personnel with cyber-security responsibilities complete role-based training, or shutting down the system.

5.11.2 Apply Security Patches and Upgrades

Assessment findings often indicate that a patch or upgrade is available for vulnerable system components that, when applied, will remediate identified weaknesses. To maintain an authorization to operate and protect against the exploitation of legitimate weaknesses (e.g., malicious code insertion), system ISSOs must apply recommended patches and upgrades to vulnerable components within the timeframes established for the RA-5 control in CSO-STD-0020, "Organization Defined Values for System Security Controls."

5.11.3 Configure System Components per NRC Standards

Assessment findings often indicate that specific configuration settings should be changed to remediate identified weaknesses. To maintain an authorization to operate and protect against the exploitation of identified weaknesses, system ISSOs must apply the configuration settings established in the secure baseline configurations provided in NRC approved security configuration standards (available at (http://www.internal.nrc.gov/CSO/standards.html) within the timeframes established for the RA-5 control in CSO-STD-0020, "Organization Defined Values for System Security Controls."

5.11.4 Develop or Update Deficient System Documentation

Robust system artifacts (documentation) clearly state how the system is implementing a specific control, provide details concerning system-specific policy, and provide detailed system-specific procedures. If, during a security control assessment, the assessor determines that system documentation had not been developed, is out of date, or is inaccurate, the system ISSO must ensure that the associated finding is remediated by developing or updating the documentation to address the issues. For example:

- If the assessor finds the System Security Planning control (PL-2) to be deficient due to missing information concerning the implementation of security controls for a specific application, the system ISSO must ensure that details concerning the implementation of the controls for the application are provided.

- If the assessor finds the Configuration Management Information System Component Inventory control (CM-8) to be deficient due to incorrect information for hardware and software components, the system ISSO must ensure that missing components and/or information are listed in the inventory, and that the information is correct.

5.11.5 System Deviations/Waivers

When the system owner is not able to mitigate a weakness within the timeframe required by CSO-STD-0020, the system owner must request a deviation/waiver for the DAA to accept the risk of not mitigating the weakness within the timeframe. All deviations/waivers must be reviewed at least annually to determine whether or not the rationale for accepting the risk still exists. For example, if a patch was released after the DAA accepted the risk, the rationale for accepting the risk of the weakness is no longer valid.

The intent of a deviation/waiver request is to ask the DAA to accept the risk posed by operating a system with an identified security issue. The ISSO must evaluate every weakness identified for the system, carefully considering the current threat environment and the weakness' inherent risk to the organization. For some weaknesses, there may be driving factors that prevent a weakness from being remediated. In these cases, the ISSO and system owner must respond to the finding by developing a deviation/waiver request and submitting the request to the DAA per the requirements established in CSO-PROS-1324, "System Deviation/Waiver Process."

The CISO shall review the request and provide a recommendation to the DAA concerning the request. The DAA will then formally notify the system owner if a decision is made to accept the risk.

All findings must be tracked within the system POA&M as open (unresolved) weaknesses until they are remediated or the DAA formally accepts the risk.

System ISSOs must track all identified findings and the plan for remediating the findings in the system POA&M per CSO-PROS-2016, "Plan of Action and Milestones Process."

A history of regular POA&M maintenance demonstrates that an organization is proactive in planning for the remediation of identified findings and reporting the security state of its systems to organization officials on an ongoing basis. Therefore, in addition to the NRC required quarterly POA&M updates, it is strongly recommended that system ISSOs maintain system POA&Ms as changes to milestones occur.

5.12 Information System Removal and Disposal

For systems no longer required for NRC use, the system owner must ensure CSO-PROS-2101, "NRC IT System Decommissioning and Disposal Process" is followed.

5.13 System Changes

The system's authorized secure and hardened baseline configuration shall be maintained through a disciplined configuration change control process. System changes must be coordinated with CSO as indicated in CSO-PROS-1321, "System Cybersecurity Coordination Process for New Systems and System Changes." Until this process is issued, system changes must be coordinated from system change project kickoff through continuous monitoring at major project management milestones with project management cybersecurity relevant deliverables.

An effective configuration change control process must include the following for all types of changes:

- Systematic documentation, proposal, justification, test/evaluation of change in non-production environment, review, approval, implementation, and disposition of changes to the system;
- Analysis of changes to the system to determine potential security impacts prior to change implementation;
- Consultation with NRC CSO prior to implementing any changes to the system that have a cybersecurity impact. Depending on the type of change, re-authorization may be required. Examples of changes to the system that have a cybersecurity impact include but are not limited to:
  - Changes to system boundary
  - New system interconnections
  - Changes to system hardening (e.g. ports, protocols, services, etc.)
  - Introduction of new products and/or technologies
  - Major upgrades or platform changes (hardware or software)
  - Addition/removal/modification of one or more security controls
  - Changes in physical environment controls or location
- Approval of all changes by a chartered Configuration Control Board (CCB), which includes CSO membership and approval authority;
- Use of NRC-approved change and configuration management tools for tracking system changes;
- Retaining records of configuration-controlled changes to the system;
- Routine auditing of changes by independent party (e.g. Independent Verification & Validation (IV&V));
- Updating system documentation of baseline configuration (e.g. system architecture document, documented configurations, operational support guide, system security plan, system inventory, etc.) to reflect approved changes. Document the specific changes to the hardware, software, or firmware such as version or release numbers, descriptions of new or modified features/capabilities, and security implementation direction; and
- NRC DAA authorization to implement the change prior to placement into operation or use with real data.

5.13.1 Identify Proposed Changes

One of the first steps in changing a system is for the system owner to provide the proposed changes to CSO for evaluation of cybersecurity.

If a change is readily identifiable as a minor change using CSO-STD-6001, “System Change Significance Standard,” the system owner is authorized to make the change and implement upon CCB approval. The system owner must follow the CSO-STD-6001 requirements to notify CSO, and system documentation must be updated to reflect the change. Until CSO-STD-6001 is issued, CSO staff will determine if a change is minor on a case by case basis.

If the change is not a minor change, change coordination should follow CSO-PROS-1321.

5.13.2 Determine Security Impact of Changes

Levels of system change are differentiated between one another with respect to the severity of the change and associated level of security impact to the system or to other systems. Sometimes a change to one system may have an impact on the security posture of another system. More significant changes have a greater impact to the security posture of systems and less significant changes may have little or no impact to the security posture of systems. The more significant the change, the more likely that a system or subsystem re-authorization effort may be required in order to fully determine the risk associated with the changed system. Changes to a system may impact other network components or interfacing systems as well as the changed system.

CSO-STD-6001, "System Change Significance Standard," provides requirements to determine the significance of a proposed change to an authorized NRC system, including its environment of operation. CSO evaluates the proposed change using CSO-STD-6001, and determines the potential impact the change may have on the system security posture, other system's security posture, and the agency's security posture. Based upon the assessment of the change, CSO can require:

- A complete system or subsystem re-authorization process;
- A partial system or subsystem assessment (see section 5.13.3); or
- Standard change testing, using system test methodologies.

The remaining system change sections are followed if a partial system or subsystem assessment is required.

5.13.3 Assess Changed System

An independent assessment of the security controls impacted by the change must be performed and an assessment report generated.

5.13.4 Remediate Assessment Findings

All findings from the assessment must be addressed and remediated. This must be accomplished in accordance with NRC processes and requirements, but, if possible, prior to change implementation.

5.13.5 Update System Documentation

System documentation must be updated to reflect the change prior to change implementation.

Per NIST SP 800-137:

> When updating key information in security plans, security assessment reports, and plans of action and milestones, organizations ensure that the original information needed for oversight, management, and auditing purposes is not modified or destroyed. Providing an effective method of tracking changes to information over time through strict configuration management and control procedures (including version control) is necessary to: (i) achieve transparency in the information security activities of the

organization; (ii) obtain individual accountability for security-related actions; and (iii) better understand emerging trends in NRC's information security program.

5.13.6 Submit Change Documentation to DAA for Authorization to Operate

System changes other than minor changes must be authorized by the NRC DAA, and the NRC DAA must accept the risk associated with the change.

6 CONTINUOUS MONITORING OF OTHER AGENCY SYSTEMS USED BY NRC

NRC uses systems owned and/or operated by other agencies. These systems require an NRC system owner and must be authorized for NRC use by the NRC DAA, and must request authorization using CSO-TEMP-1325, "Authority to Use Request Memo." NRC system owners for systems owned and/or operated by other agencies (e.g., eGovernment systems) must ensure that these systems also satisfy the annual requirements and have a valid ATO issued by the other agency. For such systems, the NRC system owner must:

1. Verify that day-to-day security operations of the interconnected system(s) are carried out including periodic vulnerability assessment scanning, annual CP testing and annual control testing.

2. Submit evidence of the execution of annual contingency plan testing and annual security control testing to the CSO within one year and one month of the previous test report date.

3. Ensure that terms of any applicable Memorandum of Understanding (MOU), Interconnection Security Agreement (ISA), and Authority to Use (ATU) are reviewed at least annually and are carried out accordingly. Enter the most recent MOU and ISA in ADAMS as an OAR and submit to CSO by emailing the ADAMS accession number to RidsCsoMailCenter Resource at least annually no later than 60 days after the date of the last signature.

4. Ensure that the sponsoring agency maintains the system ATO in accordance with NIST Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.

5. Ensure that the system maintains its authorization granted by the NRC DAA, and is re-authorized by the NRC DAA upon any significant change that might give rise to additional/other risks.

6. Notify the DAA for non-major IT investments of an ATO expiration or termination, significant changes, unacceptable risks or any changes to the MOU/ISA at least 30 calendar days in advance of such events.

7. Ensure the system has a formal ATU granted by the NRC DAA for non-major IT investments.

7 PERIODIC REVIEWS AND RISK MANAGEMENT STATUS REPORTS

Periodic reviews of offices and regions and their systems are conducted by the CSO to provide senior officials with an NRC-wide view of the agency's cybersecurity posture. The results of these reviews are provided to the Deputy Executive Directors for Operation (DEDO) and are

reflected on the CRDB. The purpose of the periodic reviews is to provide System Owners and the NRC DAA with the status of the security posture of offices, regions, and systems; recommendations for security posture improvement; and the progress made by each office and region in satisfying continuous monitoring requirements. These requirements are essential to support the overall cybersecurity risk management activities of the NRC and the continued acceptance of any residual risk during operation.

Systems are evaluated to verify the timely completion of the continuous monitoring requirements described in this document.

8 CYBERSECURITY INCIDENTS

Office directors and regional administrators must ensure appropriate counseling is provided upon staff unauthorized releases of information and other staff generated cybersecurity incidents. Repeat offenders may be subject to agency stipulated consequences. Cybersecurity incidents must be reported to the NRC Computer Security Incident Response Team (CSIRT) at 301-415-6666 or via email at CS_IRT@nrc.gov.

When a system breach occurs, the breach must be reported to the CSIRT and investigated. A breach indicates a failure of a cybersecurity control. The cybersecurity controls identified in the breach analysis as reasons for the success of the breach must be addressed in the system POA&M as POA&M items to be mitigated.

Security breaches in other agency systems used by NRC that may impact NRC information must also be reported to CSIRT.

9 SIGNIFICANT CONCERNS

This section provides the thresholds for informing agency officials of significant concerns regarding the security state of systems.

Independent assessors must ensure that all significant concerns indicating potential risk to NRC (identified during security control assessments, vulnerability scans, and configuration checks of system components) are immediately (within 24 hours) communicated to the system ISSO.

The system ISSO must ensure that significant concerns indicating potential risk to the system organization, business area, or agency are communicated to the system owner and appropriate agency official (or officials) per the official's responsibilities as documented in Management Directive 12.5, "NRC Cyber Security Program."

Examples of significant concerns that must immediately be communicated to the system owner and CISO include, but are not limited to:

- The ineffective implementation of critical controls (i.e., controls associated with SANS Critical Security Controls, available at http://www.sans.org/critical-security-controls). Examples include, but are not limited to:
  - Out-of-date malware signatures.
  - Web application vulnerabilities that could allow an attacker to gain control over vulnerable machines (e.g., cross-site scripting).

  - Backup and/or failover capabilities that are not sufficient to continue critical agency operations or recover critical agency data in the event of a contingency.
  - Personnel with technical security responsibilities (e.g., system administrators) that are not adequately trained.
  - Security incidents that have not been reported to the CSIRT, or evidence that the organization is not following agency incident response process.
- Non-compliance with federal legislation and regulations, (e.g., FIPS).
- Non-compliance with agency directives, policies, processes, procedures, standards, and guidelines.
- A change to the system or environment of operation that has not been authorized.
- Obstacles that prevent ongoing awareness of the current security state of the system and system components and near real-time risk management.
- Persistent recurrence of the same or similar findings over time, indicating that vulnerabilities are not being consistently remediated. If the finding has been identified by the Cyber Situational Awareness, Analysis, and Response (CSAAR) SITSO as a potential exploit that impact a system under the ISSO's responsibility and requires prioritized patching sooner than the NRC required timeframe.
- For systems that process PII, the PII on the system is not adequately documented and/or the system is not effectively protecting the PII. This must also be communicated to the NRC Chief Privacy Officer.
- A large number of vulnerabilities (e.g., scan findings) that present an aggregate risk that is unacceptable to the NRC.

10 CSO REPORTING

CSO provides available cybersecurity risk relevant data on the agency-wide CRDB. The CRDB top level is open to all NRC internal network users. Details for systems are restricted to those with a need to know the information, including office directors, their deputies, and above; the system ISSOs; system management; and CSO staff.

10.1 Significant Issues

When significant issues are identified, CSO staff reach out to system representatives to ensure they are aware of the issues. If issues become more significant or are not addressed in a reasonable and timely manner, they are raised to higher management levels of system responsibility. When communicating significant issues via email, CSO will digitally sign the e-mail using the CSO staff member private authentication key so that recipients can verify that the email was sent by the CSO staff member. If the electronic communications are sensitive, the CSO will encrypt the email using the public encryption key of the ISSO.

10.1.1 System ISSO

The system ISSO is the first system representative to be notified about an issue. CSO staff attempt to directly contact the ISSO verbally to ensure the ISSO is aware of the issue and then follows up with an email describing the issue to be resolved. The ISSO is provided with a reasonable amount of time to begin addressing the issue and bring it to resolution. If progress

and ultimate resolution of the issue is not achieved in a reasonable amount of time, the issue is escalated to the manager (branch chief or above) of the system ISSO.

10.1.2 Manager of System ISSO

The manager of the system ISSO provides direction and resources to the system ISSO.

If progress and ultimate resolution of the issue is not achieved by the system ISSO in a reasonable amount of time, CSO staff attempt to directly contact the manager of the system ISSO verbally to ensure the manager is aware of the issue and shall then follow-up with an email describing the issue to be resolved. The manager is provided with a reasonable amount of time to begin addressing the issue and bring it to resolution. If progress and ultimate resolution of the issue is not achieved in a reasonable amount of time, the issue is escalated to the division director of the system ISSO.

10.1.3 Division Director of System ISSO

The division director of the system ISSO has responsibility for allocating time, resources, and funding to the system ISSO to perform ISSO tasks.

If progress and ultimate resolution of the issue is not achieved by the manager in a reasonable amount of time, CSO staff shall attempt to directly contact the division director of the system ISSO verbally to ensure the division director is aware of the issue and shall then follow-up with an email describing the issue to be resolved. The division director is provided with a reasonable amount of time to begin addressing the issue and bring it to resolution. If progress and ultimate resolution of the issue is not achieved in a reasonable amount of time, the issue is escalated to the system owner.

10.1.4 System Owner

If progress and ultimate resolution of the issue is not achieved by the division director in a reasonable amount of time, CSO staff shall attempt to directly contact the system owner verbally to ensure the system owner is aware of the issue and shall then follow-up with an email describing the issue to be resolved. The system owner is provided with a reasonable amount of time to begin addressing the issue and bring it to resolution. If progress and ultimate resolution of the issue is not achieved in a reasonable amount of time, the issue is escalated to the DAA.

10.1.5 DAA

If progress and ultimate resolution of the issue is not achieved by the system owner in a reasonable amount of time, CSO shall provide the DAA with a briefing on the issue. Depending upon the nature of the issue, the DAA may:

- Determine that the DAA will accept the risk of operating with the issue
- Determine that funding should be re-allocated to address the issue
- Require a full or partial system reauthorization due to:
  - a significant change to the system or the system's environment of operation.
  - the deficient implementation of specific security controls.
  - changes to specific aspects of the system that are not deemed to be significant.

- Require a full or tailored security control assessment due to events that occurred during the quarter that warrant an immediate need to assess the effectiveness of specific security controls. For example:
  - Ineffective Access Controls. For example, accounts were identified with excessive permissions, mechanisms are not in place to control the flow of information within the system and between interconnected systems, logical access to information and system resources is not enforced, or remote access to the system is not monitored.
  - Ineffective Audit and Accountability Controls. For example, audit records do not capture the information required to support non repudiation, insufficient storage capacity is allocated for audit records, or audit records are not generated for key system components.
  - Ineffective Configuration Management. For example, the system inventory is inaccurate or incomplete, the baseline configuration is out of date, changes to the baseline configuration are not controlled, or system backups are not conducted in a manner supporting the recovery and reconstitution of the system.
  - Ineffective Identification and Authentication. For example, a weak level of authentication is used for network access to privileged accounts, the authentication mechanism is not replay resistant, system components are not uniquely identified and authenticated before establishing local, remote, and network connections, or the system authenticates to a cryptographic module that is not certified as FIPS 140-2, “Security Requirements for Cryptographic Modules” compliant.
  - Ineffective Vulnerability Management. The lack of a formal, documented patch and vulnerability management processes for a system may indicate that patches and updates are not applied per NRC requirements.
  - Ineffective System and Communications Protection. For example, cryptographic mechanisms used within the system authorization boundary are not certified as FIPS 140-2 compliant, or inadequate boundary protection is not in to ensure that the system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.
  - Ineffective System and Information Integrity. For example, malicious code protection mechanisms have not been implemented, user input is not validated per agency requirements, or information stored on and generated by the system is not handled in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
  - Inconsistent compliance with agency required continuous monitoring activities. For example, a significant number of unremediated weaknesses have been identified that are not being tracked in the system POA&M or vulnerability scanning and configuration checks of system components have not been conducted per agency sampling requirements and monitoring frequencies negatively impacting the overall security state of the system.

10.2 Quarterly Briefing to the DAA

The CISO briefs the DAA for Major IT Investments quarterly concerning the security state of NRC systems. The briefing materials focus is on agency-wide issues or trends as well as specific system issues that pose a risk to the NRC and recommendations for improving the security posture. The DAA approves or modifies the recommendations. The approvals are tracked and managed with the appropriate system owners.

Issue specific briefings to the DAA for Major IT Investments are provided on an as-needed basis.

APPENDIX A ACRONYMS

ADAMS	Agencywide Documents Access and Management System
ASCA	Authorization System Cybersecurity Assessment
ATO	Authority to Operate
ATU	Authority to Use
BARA	Business Area Risk Assessments
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Plan
CRDB	NRC Cybersecurity Risk Dashboard
CSAAR	Cyber Situational Awareness and Incident Response
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Office
DAA	NRC Designated Approving Authority
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
EDO	NRC Executive Director for Operations
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
IAT	Independent Assessment Team
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring

ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute for Standards and Technology
NRC	United States Nuclear Regulatory Commission
OAR	Official Agency Record
OIS	Office of Information Services
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCT	Policy Compliance and Training
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
PSCA	Periodic System Cybersecurity Assessment
RMF	Risk Management Framework
SA	System Administrators
SAR	Security Assessment Report
SCAP	Security Content Automation Protocol
SGI	Safeguards Information
SITSO	Senior Information Technology Security Officer
SLA	Service Level Agreement
SO	System Owner
SP	Special Publication
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team

APPENDIX B GLOSSARY

Authorization System Cybersecurity Assessment (ASCA)	A full cybersecurity control assessment of the system or subsystem that supports an authorization decision.
Business Area Leaders	A business area leader is an office director, a regional administrator, or a deputy executive director responsible for an NRC business area, such as nuclear reactor regulation. A business area leader has inherent Government authority, must be a Government employee, and is responsible for the following as it relates to cybersecurity: a. Identifying mission, business, operational requirements, and IT resources necessary for the business area to support the mission and for compliance with cybersecurity requirements; b. Identifying resources required for critical business processes and determining the impact of unavailability of those resources; c. Performing a business area risk assessment; and d. Developing a business continuity plan (BCP) for the business area.
Common Security Control	A common control is a security control that is inherited by one or more IT systems. Because common security controls protect multiple organizational systems of differing impact levels, the controls are implemented with regard to the highest impact level among the systems.
Common Security Control Provider	An office director, regional administrator, or OIS division director with overall responsibility for the development, implementation, assessment, and monitoring of a set of common controls. Common control providers, as the system owners for these systems, are accountable for the security risk associated with operating his/her system/common controls. The common control provider is an agency official who has inherent U.S. Government authority and must be a Government employee.
Hybrid Security Control	A security control that is implemented for an NRC system in part as a common security control (or inherited from another system) and in part as a system-specific security control.
Hybrid Security Control Provider	The hybrid security control providers are office directors or regional administrators with responsibility for NRC-wide parts of security controls that are partially implemented at the NRC level and partially implemented at the system level. They are responsible for the development, implementation, assessment, and monitoring of the NRC-wide portion of the controls and are held accountable for the security risk associated with operating the NRC-wide portion of the security controls.
Information Owner	Provides requirements to IT system owners regarding the security controls for the IT systems where the information resides. The information owner is an agency official who has inherent U.S. Government authority and must be a Government employee.
Periodic System Cybersecurity	A cybersecurity control assessment of the system that occurs on a

Assessment (PSCA)	periodic basis and supports continuous monitoring requirements.
Standalone Laptop, Tablet, and Personal Computer	A standalone device is one that is not connected to any other computer or to a network.
System Owner	An office director, regional administrator, or OIS division director that has overall responsibility for the security of NRC systems owned by his or her organization or operated on behalf of his or her organization by another agency or by a contractor. The system owner is an agency official who has inherent U.S. Government authority and must be a Government employee.
Tier 1 Metrics	Directly support agency-wide information security governance risk management decisions. Tier 1 metrics are provided to the Tier 1 officials during DAA risk briefings and via the NRC Cybersecurity Risk Dashboard (CRDB).
Tier 1 Officials	The NRC Designated Approving Authorities (DAAs), including the Major IT Investments DAA and the Non-Major IT Investments DAA. Each NRC DAA is a committee of individuals appointed by the NRC Executive Director for Operations (EDO).
Tier 2 Metrics	Identify issues that impact mission or business processes. Tier 2 metrics are provided to the Business Area Leaders via Business Area Risk Assessments (BARAs) and the CRDB.
Tier 2 Officials	Business Area Leaders (Business Line Managers)
Tier 3 Metrics	Identify issues with systems; provided to the Tier 3 officials via Chief Information Security Officer (CISO)-tier 3 official meetings, BARAs, and the CRDB. Activities and metrics from the Tier 3 level support risk decisions made at the Tier 1 and Tier 2 level.
Tier 3 Officials	System owners, information owners, and common/hybrid control providers.

CSO-PROS-1323 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
18-Sep-09	1.0	Initial Issuance		
11-Jan-10	1.1	Revisions to reflect feedback from ASLBP review and Gartner comments and November 2009 revision to NIST SP 800-37 / CSO staff and risk-based scoring method		
06-Apr-10	1.2	Revisions to reflect CISO and SITSO comments / CSO staff		
25-Jun-10	1.3	Revised to incorporate CSO comments from concurrence meeting		
09-Jul-10	1.4	Revised criteria and scoring methodology based on lessons learned from previous review, replaced letter grade with color grade, added criteria ID numbers, and provided more directions for document updates.		
19-Aug-11	1.5	Revised CM plan criteria to remove reference to plan update and minor edits for clarification.		
24-Nov-14	2.0	Revised to reflect current continuous monitoring requirements	CSO web page and email distribution to ISSO forum	As needed