Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Process

Office Instruction:	**CSO-PROS-1323**
Office Instruction Title:	**Information Security Continuous Monitoring Process**
Revision Number:	**2.3**
Effective Date:	**June 15, 2018**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO**
Description:	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 the NRC.

Office Owner	
Primary	**Agency Official**
OCIO/CSO	Jonathan Feibus Chief Information Security Officer (CISO)

Table of Contents

Computer Security Process
CSO-PROS-1323

Information Security Continuous Monitoring Process

1 PURPOSE

CSO-PROS-1323, “Information Security Continuous Monitoring Process,” defines the information security continuous monitoring (ISCM) strategy and requirements that must be followed to maintain authorizations of Nuclear Regulatory Commission (NRC) information systems (including the Regions and the Technical Training Center [TTC]) storing or processing NRC information up to, and including, the Safeguards Information (SGI) level. The direction in this document applies to all ‘’NRC systems operated and maintained by contractors, cloud-based systems, FedRAMP systems, and any other non-NRC federal agency systems partially managed by NRC. This process also pertains to third party external IT services (EITS) provided by a cloud service provider or another government agency where NRC has no technical responsibility to maintain the service.

The ultimate objective of the continuous monitoring program is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates. ISCM facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. Security controls, evolving threats and response to new vulnerabilities are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect NRC information. An effective risk management program and related continuous monitoring (CM) activities, support the shift from a static snapshot of an NRC systems’ security posture to a near real-time, dynamic security status.

The information contained in this document is intended to be used by system owners and Information System Security Officers (ISSOs) to ensure effective system level continuous monitoring activities are performed to support the NRC continuous monitoring strategy. This also assists the Computer Security Organization (CSO) in implementing the NRC Cybersecurity Program as defined in Management Directive MD 12.5, “NRC Cyber Security Program.”

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, “Enhancing the Security of Federal Information and Information Systems,” and NIST 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” the NRC ISCM program addresses how the agency conducts ongoing authorizations of NRC systems and the environments in which those systems operate, including external IT services. Information obtained through ISCM activities provides NRC with risk information that is critical for risk management decisions regarding system changes, system authorizations, budget priorities, and activity priorities.

Furthermore, the Risk Management Framework (RMF) developed by NIST Special Publication (SP) 800-37, as amended, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" describes continuous monitoring as a disciplined and structured process that integrates information security and risk management activities into the system development life cycle once authorization has been granted. Through the employment of comprehensive continuous monitoring processes, critical information is updated on an ongoing basis, which provides the Authorizing Official (AO), system owners and ISSOs with an up-to-date status of the security state of NRC systems and environments of operation.

NIST 800-37 describes an agencywide approach to continuous monitoring that supports risk-related decision making at the following tier levels:

- NRC Governance Level (Tier 1)
- Mission/Business Processes Level (Tier 2)
- Information Systems Level (Tier 3)

2.1 NRC Governance Level: Tier 1

Tier 1 ISCM risk activities relate to the agencywide governance structure that addresses agencywide risk, including core mission and business functions. ISCM, at the Tier 1 level, defines how NRC assesses, monitors, and mitigates risk on an ongoing basis, including agency oversight, to ensure the strategy is effective.

Types of risk of concern to the agency at Tier 1 would include:

- Program/acquisition risk (cost, schedule, performance)
- Compliance and regulatory risk
- Financial risk
- Legal risk
- Operational (mission/business) risk
- Political risk
- Project risk
- Reputational risk
- Safety risk

As part of the overall governance structure established by the agency, the risk management strategy is disseminated to personnel with programmatic, planning, developmental, acquisition, operational, and oversight responsibilities.

2.2 Mission/Business Process Level: Tier 2

Tier 2 addresses risk from a mission and business process perspective as guided by decisions made at the Tier 1 level. 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 defined in MD 12.5, “NRC Cybersecurity Program.” The Chief Information Security Officer (CISO) has overall responsibility for the NRC Cybersecurity Program and ensures that risk acceptance decisions are consistent across the agency. The CISO and Business Line Leads work together to determine the level of risk tolerance with respect to their business areas and the Cybersecurity Program respectively.

2.3 Information System Level: Tier 3

Tier 3 addresses risk from an information system perspective and is guided by the risk decisions at Tier 1 and Tier 2. Risk decisions at Tiers 1 and 2 impact the selection and deployment of security controls and safeguards at the system level. System owners must ensure that security controls are in place, operating as intended, and having the desired effect. Tier 3 officials include system owners, information owners, and common/hybrid control providers.

The system owner is responsible for the security of an NRC IT system and is accountable for the security risk associated with operating the system. A system owner is an office director, regional administrator, or an Office of the Chief Information Officer (OCIO) division director that has overall responsibility for the security of NRC systems owned by the organization or operated on behalf of the organization by another agency or by a contractor. The system owner must develop and maintain a continuous monitoring of system controls, in compliance with agency requirements, to maintain an understanding of the effectiveness and status of the cybersecurity control. To maximize communication and facilitate security planning, system owners must appoint a primary and alternate system ISSO as their security representatives for the system via memorandum using CSO--TEMP-0001, “System_ISSO_Appt_Email_Memo_V2.0.”

Continuous monitoring tasks cannot be achieved through manual processes or automated processes alone. While many CM tasks require human interaction, automated solutions are preferable in order to reduce the cost and effort, resulting in more frequent data (real-time) and the ability to adjust security controls based upon new threats and vulnerabilities. Tools used to support cybersecurity risk assessment must be constantly evaluated to ensure the tools are assessing the risk based upon NRC requirements.

3 SPECIFIC REQUIREMENTS

CSO--PROS-1323, “Minimum Required Frequencies for Continuous Monitoring Activities” is the companion document to this process and defines the timeframes for continuous monitoring requirements for NRC systems, EITSs, and third party EITSs.

3.1 Initial Authorization/Re-authorization

System owners must obtain an authorization before placing a system into the operational environment or using that system in any way for NRC purposes. All NRC IT resources must belong to an NRC IT system, and must therefore be part of a system authorization before being placed into operation. This includes all new systems and modifications to existing systems. To maintain a system authorization, the system owner must conduct continuous monitoring activities and ensure that the system adheres to any specified authorization conditions.

At any point in time, the AO can require that a system/subsystem undergo a re-authorization or an ad hoc (periodic) assessment effort. 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.

3.2 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 effort.

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.

3.3 System Change Authorization

Except for minor changes, system changes must have a change authorization prior to deploying to the production (NRC-managed network) environment following the Configuration Control Board (CCB) approval process and using the agency's automated change control tool. OCIO-CCB-0001, "System Change Significance Determination Process," defines the process by which the CCB determines the change significance, both business and cybersecurity, to authorized NRC systems and its operating environment. The CCB has been delegated the authority to determine the risk significance of proposed changes (both pre-production and production) and has been authorized by the AO to approve change requests determined to be of minor or moderate significance as long as the change meets the requirements outlined in OCIO-CCB-001.

Change significance depends on the severity of the change and the associated level of potential adverse security and/or business impact to a system. The greater the change significance, the more likely that a system or subsystem reauthorization effort may be required. Any changes outside the authority of the CCB will be processed by the Computer Security Organization (CSO) Point of Contact (POC) for the affected Federal Information Security Management Act (FISMA) system through the AO. Additional information can be found in OCIO-CCB-0002, "Change Approval Process."

For NRC systems that are not on the NRC-managed network (contractor sites, Regional office-network components) the ISSO must notify the CSO POC and CISO by email of the proposed system change prior to implementation.

Under certain circumstances, **a short-term authorization** is granted for a specified amount of time while testing is completed, documentation is created in order to prepare for a full authorization. It is subject to an architectural review and approval by 2 enterprise assessors.

A pilot authorization is granted for a specific period of time, with a limited number of users, while technology is tested in the production environment.

Continuous monitoring activities are **NOT** required for these types of authorizations.

3.4 Authorization of Standalone IT Resources

All NRC standalone IT resources must belong to an authorized system. Standalone IT resources can be integrated into an authorized system as part of a system change effort or during a periodic system cybersecurity assessment (PSCA). Once approved, the standalone IT resource will be incorporated into the system's continuous monitoring process.

3.5 Authorization of External IT Services

NRC system owners and office POCs must obtain authorization from the AO in order to use an IT service where the delivery of services is provided by an external organization or service provider. System owners must ensure that the external IT service provider has already obtained a valid, current authorization issued either by another government agency or through the Federal Risk and Authorization Management Program (FedRAMP) for cloud solutions. The NRC will not issue an authorization for an external IT service without a valid authorization. CSO-PROS-1325, "External IT Service Authorization Process," provides the process that must be followed to obtain authorization to use an external IT service being used in the NRC environment. External IT services include, but are not limited to, cloud computing through a cloud service provider (CSP) and interconnection with an IT system that is owned and operated by another government agency or third party provider including public facing web applications.

4 CONTINUOUS MONITORING REQUIREMENTS FOR NRC INFORMATION SYSTEMS

Once an authorization has been granted, the information system moves to monitoring phase of the Risk Management Framework.

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.

4.1 Periodic System Cybersecurity Assessments

To satisfy annual FISMA security control assessment requirements, PSCAs are conducted at least annually to determine an information system's compliance with defined security requirements in an environment of sophisticated and changing threats. The frequency of a PSCA is based on the system's authorization state and the NRC's determination of:

- the volatility of each control (the likelihood of the control changing over time subsequent to its implementation),and

- the criticality of the function supported by each security control.

CSO-PROS-2102, “System Cybersecurity Assessment Process,” defines the process that must be followed to conduct a system cybersecurity assessment of an NRC system. The system’s security categorization must be reviewed at least annually to ensure proper identification of all information types and ensure any changes to the authorization boundary have been documented. In addition, the Privacy Threshold Analysis/Privacy Impact Assessment must be reviewed at least annually to ensure proper protection of the agency’s personally identifiable information.

4.2 Vulnerability and Configuration Compliance Scans

Regular vulnerability scanning allows an ISSO to determine whether the security controls implemented to protect their system from known exploits and threats continue to be effective. Automated scanning tools are available that seek out any weaknesses (based on known security flaws, missing patches/updates), test system components and hosted applications to determine whether the flaws exist, and then generate a report of any detected weakness that will need to be remediated. 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. 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. 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 remediation must be performed in accordance with CSO-PROS-1401, “Periodic System Scanning Process,” and in accordance with the continuous monitoring requirements. System ISSOs must conduct remediation within the timeframes established for the RA-5 control in CSO-STD-0020, “Organization Defined Values for System Security Controls.”

A history of regular vulnerability scans (and the timely remediation of identified weaknesses) demonstrates that an NRC office 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 AO approval via the deviation process CSO-PROS-1324, NRC Deviation Request Process.”

4.3 Maintain System Security Documentation

System ISSOs must routinely maintain the system security documentation that provides 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 security documentation, including policies and procedures, demonstrates that an organization is proactive. All system security documentation must be maintained in accordance with NRC frequency requirements as defined in CSO-PROS-1323, "Minimum Required Frequencies for Continuous Monitoring Activities." All system security documentation must be developed and maintained in accordance with NRC-issued templates (available at https://usnrc.sharepoint.com/teams/OCIO-CSO/CSO_FISMA_Repository/Forms/AllItems.aspx?RootFolder=%2Fteams%2FOCIO%2DCSO%2FCSO%5FFISMA%5FRepository%2FCybersecurity%5FIssuances%2F07%5FTemplates&FolderCTID=0x0120004216552C6363F947AAAFBC8D4ACE675B&View=%7BD0DCAE9B%2D1A35%2D4F35%2DAC76%2DDA1DE100D61E%7D

CSO-PROC-2104, "System Artifact Examination Procedure" provides the examination criteria to be applied to each documentation artifact to ensure completeness.

4.4 Maintain System POA&Ms

CSO-PROS-2016, "Plan of Action and Milestones Process," defines the process that must be followed to identify, track, prioritize and report the status of security weaknesses identified within NRC systems including those operated by or on behalf of the NRC. The purpose of a POA&M is to assist the agency in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found during testing/monitoring activities.

POA&Ms must be reviewed and maintained quarterly by the system ISSO to ensure that identified milestones are completed by the scheduled completion dates. In addition, POA&Ms must be updated whenever activities take place that either identify new weaknesses, or demonstrate that weaknesses have been remediated.

4.5 Remediate Authorization Conditions

Any concerns that were listed in the authorization email must be noted in the system's POA&M and remediated within the timeframe that was documented in the email.

4.6 Test the System's Contingency Plan

Contingency Plan (CP) testing validates recovery capabilities, identifies potential weaknesses in the CP and improves the overall organizational preparedness to execute the plan. An annual contingency test provides assurance that the plan remains current with system and organizational changes. CP Test Report must be submitted before the date of the system's last CP Test Report.

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:

- Review and update the Business Impact Analysis (BIA) as needed
- Develop a Contingency Test Plan for testing the CP
- Conduct annual CP training for staff with contingency planning roles and responsibilities
- Coordinate testing with affected organizations
- Execute CP testing according to the Contingency Test Plan
- Develop a Contingency Test Report to document the results of testing
- Ensure that weaknesses identified through CP Testing are incorporated into the system's POA&M, as applicable

System ISSOs must document contingency plan test results using CSO-TEMP-2024, "Contingency Test Report Template", and update the contingency plan as required based upon the contingency test results.

4.7 Security Reviews and Risk Management Status

Periodic reviews of NRC IT systems are conducted to provide senior officials with an NRC-wide view of the agency's cybersecurity posture. System Owners and the NRC AO are periodically briefed on various cybersecurity metrics, continuous monitoring progress, and identified risks. Status reports and metrics are also analyzed to determine if there are any security trends that suggest changes to the monitoring strategy may be necessary.

This information is reflected in the NRC Cybersecurity Risk Dashboard (CRDB), which in turn provides executives and their staff with the status on the security posture of their respective offices, regions, and systems. Cybersecurity risk management activities are not only required by FISMA and OMB, but support the ability of the NRC to identify, manage, and minimize risk to the agency mission. The system owner must ensure that all required continuous monitoring reporting is submitted to CSO by emailing the RidsOCIO.Resource@nrc.gov, CISO, and CSO Office POC.

The status of any upcoming continuous monitoring activities and/or incomplete activities is provided monthly by CSO and reviewed with system ISSOs and office staff at continuous monitoring status meetings.

4.8 Cybersecurity training requirements

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 before July 31st. In addition, they must ensure that personnel assigned to cybersecurity roles complete required training as defined within the Training and Awareness SharePoint site at:

https://usnrc.sharepoint.com/teams/OCIO-CSO/Training_And_Awareness/Forms/AllItems.aspx?id=%2Fteams%2FOCIO%2DCSO%2FTraining%5FAnd%5FAwareness%2F01%5FROLES.

4.9 Cybersecurity Incidents

When a system breach occurs, the breach must be reported to the NRC Computer Security Incident Response Team (CSIRT) at 301-415-6666 or via email at CS_IRT@nrc.gov. Office directors and regional administrators must ensure appropriate counseling is provided after any staff unauthorized releases of information or other staff generated cybersecurity incidents. Repeat offenders may be subject to agency stipulated consequences. As part of the FISMA 2014 requirements, NRC must provide the procedures for detecting, reporting, and responding to security incidents, including notification to Congress of any major incident including a summary report.

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.

CSO presents a cybersecurity awareness briefing to the AO and senior officials daily to discuss any new critical security vulnerabilities that may have occurred. The goal is to maintain an up-to-date awareness of any threats to NRC's IT infrastructure. Statuses for any systems that are deficient in continuous monitoring activities are also presented for comment.

5 CONTINUOUS MONITORING REQUIREMENTS FOR EXTERNAL IT SERVICES

All NRC IT resources and IT external services used by the NRC must be accounted for in an NRC authorized system. System owners must ensure the security controls NRC is responsible for are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements. Continuous monitoring activities for external IT services are proportionate to the number of NRC-specific security controls that are selected as part of the NRC baseline (i.e., the more security controls for which the NRC is responsible, the more continuous monitoring activities the ISSO will have to perform).

Continuous monitoring responsibilities will also increase if the NRC is directly responsible for managing any of the components, either within the external IT service itself (e.g., in an Infrastructure-as-a-Service [IaaS] or Platform-as-a-Service [PaaS] cloud service model) or directly within the NRC environment. NRC is not responsible for continuous monitoring for security controls that are solely provided by the external IT service provider. However, system owners are responsible for ensuring that external IT service providers comply with all continuous monitoring requirements mandated by the sponsoring government agency (i.e., the agency that issued the authorization) or with FedRAMP continuous monitoring and ongoing authorization requirements provided in the "FedRAMP Continuous Monitoring Strategy and Guide. In addition, continuous monitoring activities must be performed in accordance with this process and the frequencies identified in "Minimum Required Frequencies for Continuous Monitoring Activities Defined in CSO-PROS-1323," for all components and the processes and procedures for which the NRC system owner is at least partially responsible for managing.

The ISSO or designee must incorporate external IT services security controls information into the NRC information system's security documentation including any process and procedural documents that are necessary to facilitate NRC's implementation and usage of the external IT service.

This may include but is not limited to:

- Security Categorization Report
- Privacy Threshold Analysis/Privacy Impact Assessment
- Configuration Management Plan
- Incident Response Plan
- Documented Configurations
- System Inventory
- System Architecture Document
- Operational Support Procedures
- BIA (details can be incorporated into the parent system's BIA)
- Contingency Plan (details can be incorporated into the parent system's CP)

System Owners must also ensure that the external IT service provider is complying with all contractual obligations related to IT security and meeting all service levels as documented in the service level agreement (SLA). System owners must examine external IT service security artifacts annually to ensure that external IT service providers are compliant with applicable requirements. The NRC AO and CISO must be notified of material changes to any Memorandums of Understanding (MOU) or Interconnection Security Agreements (ISA) within 30 days.

System owners must provide CSO with an annual assertion email attesting the following:

- The external IT service provider has an active authorization and has updated the authorization package appropriately.
- The external IT service provider has provided the NRC with an up-to-date POC.
- The external IT service provider is managing risks and closing POA&Ms.
- The external IT service provider has satisfied any authorization conditions that were mandated as part of the external authorization.

Further, the assertion email must state the following:

- The NRC system owner has examined all external agreements (e.g., memorandums of understanding [MOUs], interconnection security agreements [ISAs], SLAs) and confirms that all agreements are up-to-date and that the service levels documented in the SLA are being met.

Certain external IT services may qualify to be part of the NRC's Third Party System (TPS). TPS provides the management framework for external IT services that are hosted by other government agencies, or FedRAMP-authorized cloud services where there are no IT components for NRC to manage.

Implementing external IT services into the NRC environment where there are no technical components does involve the development and testing of any 800-53 security controls managed by the NRC. In addition, continuous monitoring activities must be performed in accordance with this process and the frequencies identified in "Minimum Required Frequencies for Continuous Monitoring Activities Defined in CSO-PROS-1323," for all processes and procedures for which the system owner is responsible for.

6 METRICS

Part of the NRC ISCM strategy is to collect the security-related data required for metrics, assessments, and reporting. Metrics provide meaningful indicators of the security status across all agency tiers. Each tier monitors security metrics and assesses security control effectiveness to support tier-specific decision making.

Tier 1 metrics are developed for supporting governance decisions regarding the organization, its core missions, and its business functions.

Tier 2 metrics are developed to prioritize agencywide core mission/business processes with respect to overall goals and objectives while successfully executing the NRC security program strategy.

Tier 3 metrics address risk management from an information system perspective. Continuous monitoring activities ensure that all system-level security controls are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time.

The NRC ISCM strategy established the following performance metrics to be monitored to meet NRC and federal requirements:

- System Security Plan review and update
- Quarterly Scan Reports
- Configuration risk
- Contingency Plan review and update
- Conduct Contingency Plan Test
- POA&M review and update
    - CSO examines consolidated POA&M information to determine if there are common weaknesses/deficiencies among the NRC's information systems to analyze risk and make adjustments to the ISCM strategy.
- Business Impact Analysis review and update

- Security Categorization review and update
- PIA/PTA review and update
- System Architecture Document
- Conduct Periodic System Cybersecurity Assessment
- Computer Security Awareness Training
- Role-Based Training
- Incident Trends (Data compiled from the Security Operations Center (SOC)
- Phishing Exercise Results
- Completion of AO conditions
- Number of assets
- Number of users
- Number of privileged users
- Number of Authorized systems
- Number of NRC systems leveraging a Cloud Provider
- Number of external IT services used by NRC

The AO and senior executives make risk management decisions based on these performance metrics. The monitoring strategy is regularly reviewed for relevance and accuracy in reflecting NRC risk tolerances, correctness of measurements, applicability of metrics, and effectiveness in supporting risk management decisions.

These performance metrics are also used in providing monthly CyberScope reports to DHS, quarterly reports to DHS for FISMA metrics (M-18-02) and to fulfill Federal Information Technology Acquisition Reform Act (FITARA) scoring requirements.

Tier 3 System Level Metrics

Metric 1	Authorized NRC Systems
Description	This metric provides the number of authorized NRC systems and then presented to Department of Homeland Security on a monthly basis.
Assessment Method	Review of authorization status
Frequency	Monthly
Data Source	NRC system inventory
Reporting Format	CyberScope

Metric 2	Authorized Contractor Systems
Description	This metric provides the number of authorized Contractor systems that operate on behalf of NRC. This data is then presented to Department of Homeland Security on a monthly basis.
Assessment Method	Review of authorization status
Frequency	Monthly
Data Source	NRC system inventory
Reporting Format	CyberScope

Metric 3	Authorized Government Shared Services Provider
Description	This metric provides the number of authorized Government Shared Services Providers that NRC uses to conduct business. This data is then presented to Department of Homeland Security on a monthly basis.
Assessment Method	Review of authorization status
Frequency	Monthly
Data Source	NRC system inventory
Reporting Format	CyberScope

Metric 4	PIV Card used for Privileged Users
Description	This metric provides the number of privileged users that use their PIV card to authenticate.
Assessment Method	Review statistics of privileged users using PIV authentication
Frequency	Monthly
Data Source	Active Directory Reports
Reporting Format	CyberScope

Metric 5	PIV Card used for Non-privileged Users
Description	This metric provides the number of non-privileged users that use their PIV card to authenticate.
Assessment Method	Review statistics of non-privileged users using PIV authentication
Frequency	Monthly
Data Source	Active Directory Reports
Reporting Format	CyberScope

Metric 6	Computer Security Training Completion
Description	This metric provides the number of NRC users that participated in annual computer security training exercises to increase awareness.
Assessment Method	Data is obtained from iLearn course completions
Frequency	Metric is gathered monthly
Data Source	iLearn reports
Reporting Format	CRDB & Annual FISMA Report

Metric 7	Role-Based Training Completion
Description	This metric provides the number of NRC users with different roles that require additional role-based training to fulfill NRC requirements.
Assessment Method	Data is obtained from iLearn and internal/external course completion certificates provided to OCIO.
Frequency	Continuous
Data Source	iLearn reports
Reporting Format	CRDB

Metric 8	Phishing Exercises
Description	This metric provides the number of NRC users that fall prey and click embedded links or attachments.
Assessment Method	Phishing emails are sent to 25% of the workforce each quarter
Frequency	Quarterly
Data Source	Phishing software database
Reporting Format	PhishGuru Reports and CRDB

Metric 9	Cybersecurity vulnerabilities
Description	This metric measures the number of missing patches/updates.
Assessment Method	Pull vulnerability results from Tenable Security Center
Frequency	Monthly
Data Source	Tenable Security Center
Reporting Format	CRDB and FITARA

Metric 10	Configuration non-compliance
Description	This metric measures the number of configuration settings that are not in compliance with Security Content Automation Protocol (SCAP) validated products.
Assessment Method	Pull SCAP results from Tenable Security Center
Frequency	Monthly
Data Source	Tenable Security Center
Reporting Format	CRDB and FITARA

Metric 11	POA&M weaknesses
Description	This metric provides the number of open POA&M items per system and compares progress from the previous quarter.
Assessment Method	Data is pulled from System's POA&M spreadsheet
Frequency	Quarterly
Data Source	Data comes from various assessment efforts and scan reports.
Reporting Format	CRDB and FITARA

Metric 12	Continuous Monitoring Metrics for fully authorized systems
Description	This metric provides compliance results for various continuous monitoring requirements such as contingency testing, system security plan updates, conducting PSCAs, continuous monitoring scans, ISSO, ATO, etc.
Assessment Method	Metric calculates the degree to which continuous monitoring requirements are met.
Frequency	Continuous
Data Source	Various artifacts that are submitted to OCIO/CSO
Reporting Format	CRDB

Metric 13	Continuous Monitoring Metrics for fully authorized external systems
Description	This metric provides compliance results for various continuous monitoring requirements such as system security plan updates, conducting PSCAs, ISSO, ATO, etc.
Assessment Method	Metric calculates the degree to which continuous monitoring requirements are met.
Frequency	Continuous
Data Source	Various artifacts that are submitted to OCIO/CSO
Reporting Format	CRDB

APPENDIX A. ACRONYMS

AO	Authorizing Official
ASCA	Authorization System Cybersecurity Assessment
BIA	Business Impact Analysis
CISO	Chief Information Security Officer
CP	Contingency Plan
CRDB	Cybersecurity Risk Dashboard
CSO	Computer Security Organization
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
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	Nuclear Regulatory Commission
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
PSCA	Periodic System Cybersecurity Assessment
SCAP	Security Content Automation Protocol
SLA	Service Level Agreement

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: • Identifying mission, business, operational requirements, and IT resources necessary for the business area to support the mission and for compliance with cybersecurity requirements; • Identifying resources required for critical business processes and determining the impact of unavailability of those resources; • Performing a business area risk assessment; and • Developing a business continuity plan (BCP) for the business area.
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 Assessment (PSCA)	A cybersecurity control assessment of the system that occurs on a 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 OCIO 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.

CSO-PROS-1323 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
29-July-19	2.3	Added SAD to document requirements	CSO web page and email distribution to ISSO forum	As needed
09-May-18	2.2	Revised to include external IT services and to reflect changes to other processes and organizational structures	CSO web page and email distribution to ISSO forum	As needed
28-Sep-16	2.1	Revised to add metrics in accordance with the GAO high-risk systems audit and to reflect changes to other processes and organizational structures.	CSO web page and email distribution to ISSO forum	As needed
24-Nov-14	2.0	Revised to reflect current continuous monitoring requirements	CSO web page and email distribution to ISSO forum	As needed
19-Aug-11	1.5	Revised CM plan criteria to remove reference to plan update and minor edits for clarification.		
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.		
25-Jun-10	1.3	Revised to incorporate CSO comments from concurrence meeting		
06-Apr-10	1.2	Revisions to reflect CISO and SITSO comments / CSO staff		
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		
28-Sep-08	1.0	Initial Issuance		