Cybersecurity Risk Management Activities Instructions
Fiscal Year 2023

On December 18, 2014, to update the Federal Information Security Management Act of 2002, President Barack Obama signed into law the Federal Information Security Modernization Act of 2014 (FISMA), which strengthens the security of computer networks and information systems.

FISMA improves security by transitioning agencies away from paperwork requirements and toward a more automated and continuous security posture. FISMA maintains much of the preexisting law, including the development, documentation, and implementation of an agencywide information security program to provide security for information and support systems. FISMA applies to all systems, including national security systems. The U.S. Nuclear Regulatory Commission (NRC) designated the Cybersecurity Branch of the Office of the Chief Information Officer (OCIO) to identify and maintain the agency's information security program, with oversight provided by the Chief Information Security Officer.

FISMA requires that the NRC information security program include the following:

- periodic testing and evaluation of the effectiveness of policies, practices, and procedures, and the assessment of risk and magnitude of potential harm
- policies and procedures to cost effectively reduce information security risks based on risk assessments
- assurance that information security is addressed throughout the life cycle of each agency information system
- acceptable system configuration requirements
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the agency's information security policies, procedures, and practices
- security awareness training
- procedures for detecting, reporting, and responding to security incidents
- periodic reporting requirements

The requirement to provide procedures for detecting, reporting, and responding to security incidents includes notification of the U.S. Department of Homeland Security and the Office of Management and Budget (OMB) within 1 hour of confirmation of a major incident, as well as notification of Congress and the NRC Office of the Inspector General (OIG) no later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred.

The NRC must also submit annual reports to designated agency officials and congressional committees on the adequacy and effectiveness of its information security policies, procedures, and practices. An effective risk management program and compliance with FISMA require the

NRC to continuously monitor the security posture of its systems, mitigate vulnerabilities, and maintain accurate and up-to-date plans of action and milestones (POA&Ms). The NRC implements its enterprise risk management program and related cybersecurity risk management activities at both the agency and individual system levels.

Continuous monitoring guidance, periodic reviews, cybersecurity training requirements, and the Cybersecurity Risk Dashboard (CRDB) ensure that Office Directors and Regional Administrators are effectively managing cybersecurity risk at the agency level. At the system level, the system owners implement continuous monitoring plans that address existing cybersecurity risk management requirements to monitor changes to the system and cybersecurity controls to ensure that the system's security posture is not degraded.

Attention to security requirements is essential to minimize both risk and potential audit findings. OIG performs annual audits and documents gaps in NRC cybersecurity workforce training and contingency planning and required cybersecurity activities that are either delayed or not performed. In addition, several Government Accountability Office audits found that the NRC failed to perform required cybersecurity activities. In recent years, external auditors found that critical weaknesses were not being mitigated in a timely manner or tracked or monitored sufficiently.

1 GENERAL REQUIREMENTS

To continue efforts to streamline the document submission requirements (outlined below), all FISMA-required submissions of continuous monitoring security artifacts must be sent to CSO-FISMA-Submittals@nrc.gov, unless previously submitted through the Risk and Continuous Monitoring and Tracking System (RCATS). To provide appropriate routing guidance to the Computer Security Organization (CSO), any email submission should begin with a statement that it contains a cybersecurity continuous monitoring artifact.

These documents will be added to the SharePoint online CSO FISMA repository in the appropriate FISMA system folder or retained in RCATS, as appropriate. Use of these tools will continue to reduce the burden on the system owner staff and decrease the resources needed to comply with annual OMB and OIG FISMA audit requirements. The FISMA repository can be found at this link and RCATS at this link.

Placing documents in the Agencywide Documents Access and Management System (ADAMS) is no longer required. However, for information system security officers (ISSOs) who want to upload documents into ADAMS (documents containing security-related information should not be profiled to include all NRC users), "Viewer" access-level rights must be extended to the following groups:

- OCIO-GEMSD-ISPOB-Rev CTR
- OCIO-GEMSD-ISPOB-Rev Group
- OIG-FISMA Audit

As a reminder, classified material and safeguards information are prohibited in ADAMS. If the information relates to a classified or safeguards information system, the email should only refer the recipient to the specific location of the required information.

To promote good security practices and the best possible security posture, FISMA requires that continuous monitoring security artifacts be completed by their due dates and submitted within 10 working days of completion. This will ensure effective communication of the most accurate information and full credit during annual OIG FISMA reviews. ISSOs should coordinate with their CSO point of contact to ensure that the data are accurate and current on the CRDB and in RCATS. These tools will reflect incomplete or late submissions, which may adversely affect system and office Cybersecurity Performance Index scores reported as the AW-IT-01 metric to Office Directors, Regional Administrators, the Chief Information Officer (CIO), and the Executive Director for Operations during agencywide quarterly performance reporting reviews.

Office Directors, Regional Administrators, system owners, or their representatives should involve (as necessary) CSO, Intake, and NRC Configuration Control Board staff at the start of any initiative to develop, modernize, or enhance an information technology system. This early involvement will allow CSO, Intake, and Configuration Control Board staff and the project team to discuss requirements and options and address any documentation and process questions, thereby minimizing schedule delays and cost.

CSO periodically reviews required cybersecurity activities with system owners' staff and updates the agency's CRDB and RCATS. The system owner (or approved designee) is responsible for submitting to CSO any information that changes the status of these activities as tracked in the CRDB. The data in the CRDB are periodically reported to the Chief Information Security Officer, the CIO, Office Directors, the OIG, and system owners, as appropriate. In addition, in accordance with the Federal Information Technology Acquisition Reform Act, the CIO reviews all information technology investments monthly and performs a cybersecurity review.

2 INSTRUCTIONS FOR OFFICE DIRECTORS AND REGIONAL ADMINISTRATORS

OMB Circular A-130, "Managing Information as a Strategic Resource," issued July 2016, and FISMA require agencies to ensure that all individuals receive security awareness training and specialized training focused on their cybersecurity role and responsibilities. Office Directors and Regional Administrators are responsible for ensuring that all staff and contractors complete annual cybersecurity awareness training and that those with significant cybersecurity responsibilities complete the necessary and required role-based training.

2.1 Cybersecurity Awareness and Training

Office Directors and Regional Administrators must ensure that all staff and contractors complete the annual computer security awareness course. This course must be completed within 1 week of obtaining access to NRC electronic information and after that, no later than July 31 each year.

2.2 Cybersecurity Role Identification and Required Role-Based Training

OMB Circular A-130 and FISMA require that all personnel with significant cybersecurity responsibilities be identified and appropriately trained. The NRC definitions of significant cybersecurity roles are available at this link. Effective June 14, 2004, the Office of Personnel Management requires agencies to develop a cybersecurity training plan for those with significant cybersecurity responsibilities. The plan must include provisions for role-specific training as detailed by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, "Information Technology Security Training Requirements: a Role- and

Performance-Based Model," issued April 1998, and SP 800-50, "Building an Information Technology Security Awareness and Training Program," issued October 2003.

The Office of Personnel Management also encourages training to reflect the NIST National Initiative for Cybersecurity Education, located at this link.

The NRC cybersecurity training plan is located at this link. The current training plan will transition to include the Cybersecurity Workforce Development Plan in the near future. Office Directors and Regional Administrators must ensure that CSO and the Office of the Chief Human Capital Officer have a current list of individuals in their office or region who are assigned significant cybersecurity roles and that any change in roles is communicated within 30 working days. All Division Directors and above are considered executives and must take role-based training for executives. The current list of individuals assigned to significant cybersecurity roles can be found at this link.

A list of available courses to assist with role-based training requirements can be requested by emailing CybersecurityTraining.Resource@nrc.gov. CSO collaborates with the Office of the Chief Human Capital Officer to identify cybersecurity roles, along with required curricula, within the agency learning management tool.

Office Directors and Regional Administrators with information technology systems must appoint a primary and alternate office ISSO to represent the office (and all ISSOs within the office) to the ISSO forum and to CSO using CSO-TEMP-0002, "Office Information System Security Officer (ISSO) Appointment Template." Additional information about the ISSO forum can be found at this link or by emailing CybersecurityTraining.Resource@nrc.gov.

Offices may decide to have a single individual represent multiple offices. The appointment memorandum should indicate this. ISSO forum meetings allow ISSOs to learn about and share cybersecurity articles, research, events, trends, and incidents; current activities and initiatives; lessons learned; and best practices.

Additionally, to maximize communication, facilitate security planning, and minimize mission risk, system owners must appoint primary and alternate system ISSOs as their security representatives for the system by email using CSO-TEMP-0001, "System Information System Security Officer (ISSO) Appointment Template." 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 effective over time.

Office Directors and Regional Administrators must ensure that the following activities take place:

- Office ISSOs participate in the ISSO forum meetings, biannual all-ISSO meetings, and cybersecurity seminars.

- System ISSOs participate in the biannual all-ISSO meetings and cybersecurity seminars.

- Staff members with significant cybersecurity responsibilities complete the mandatory security-related training detailed in the NRC cybersecurity training plan (to be augmented by the Cybersecurity Workforce Development Plan upon issuance).

3 INSTRUCTIONS FOR SYSTEM OWNERS

NRC systems include those operated by or on behalf of the NRC, including all systems operated and maintained by contractors, cloud-based systems, Federal Risk and Authorization Management Program (FedRAMP) systems, and all other non-NRC Federal agency systems used by the NRC. All NRC resources related to information technology must belong to an NRC information technology system and be part of a system authorization before being operated.

Once an authorization has been granted, the authorizing official (AO) establishes the termination date and specific conditions. The AO can adjust the authorization termination date at any time to reflect an increased level of concern about the system's security and privacy posture. After a full authorization effort is complete, an ongoing authorization can be granted if the system's continuous monitoring program is sufficiently robust and mature. The AO must be provided with the necessary information to conduct ongoing risk determinations and risk acceptance or denial activities depending on the security and privacy posture of the system. At any time, the AO can require a system or subsystem to undergo a reauthorization or an ad hoc (periodic) assessment effort if continuous monitoring results adversely change the ongoing risk determination levels.

CSO-PROS-2030, "NRC Risk Management Framework (RMF) Process," defines the processes and procedures that must be followed to apply the guidelines from NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," issued December 2018, to secure NRC information systems. This document describes in detail the seven steps in the RMF process and the security tasks and documents that are required to be in alignment with NRC policy. In addition, various process documents that support the NRC RMF process are available on the CSO FISMA repository SharePoint site. They include but are not limited to the following:

- CSO-PROS-1323, "Information Security Continuous Monitoring Process"
- CSO-PROS-1323, "Frequencies Companion Document"
- CSO-PROS-1324, "Deviation Request Process," as amended
- CSO-PROS-1325, "External IT Service Authorization Process"
- CSO-PROS-1401, "Periodic System Scanning Process"
- CSO-PROS-2001, "System Security Categorization Process"
- CSO-PROS-2104, "System Artifact Examination Procedure"
- CSO-PROS-2016, "POA&M Process"
- CSO-PROS-2101, "Decommissioning-Transfer Process"
- CSO-PROS-2102, "System Cybersecurity Assessment Process"
- CSO-PROS-8001, "FITARA Cybersecurity Risk Rating and Reporting Process"

As cybersecurity artifacts are developed for system authorization requests or are updated and submitted to CSO in support of the continuous monitoring activities outlined below, system owners must ensure that these artifacts meet the minimum requirements prescribed by CSO-PROS-2104. This procedure clearly articulates NIST requirements so that system owners, their staff, and independent assessors can efficiently and consistently develop cybersecurity deliverables that will help minimize risk to the NRC mission.

3.1 Continuous Monitoring

Continuous monitoring activities for information security are part of the mandatory information security management framework defined by FISMA and the security authorization process required by OMB Circular A-130. The ultimate objective of information security continuous monitoring is constant, near-real-time risk detection and management. Continuous monitoring requirements apply to any NRC-established system, including all systems operated and maintained by contractors, cloud-based systems, FedRAMP systems, and all other non-NRC Federal agency systems used by the NRC.

System owners must ensure that all systems are authorized by the NRC AO and follow CSO-PROS-1323. NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," issued September 2011, and OMB Circular A-130 provide clear instructions for maintaining an effective risk management program for systems authorized by the NRC AO. This requirement applies to NRC-owned systems, its contractor-owned or -operated systems, and all non-NRC federally owned or operated systems that store or process NRC data. For reference, CSO-PROS-1323 identifies NRC-defined continuous monitoring frequencies and timeframes.

3.2 System Cybersecurity Assessment

As prescribed by NIST, OMB, and FISMA requirements, the purpose of the system cybersecurity assessment (SCA) is to determine the extent to which cybersecurity controls are implemented correctly, operating as intended, and producing the desired results. The assessment results are documented in an SCA report and provide insight into the current security state of a system and its associated risk. The SCA contains a list of recommended corrective actions for weaknesses or deficiencies identified during the assessment. The SCA supports risk management and helps ensure that the information system owner, common control provider, and AO maintain appropriate awareness of security control effectiveness. The overall effectiveness of the security controls directly affects the ultimate security state of the information system and decisions about the explicit acceptance of risk. All SCA results must be provided to CSO at the required frequency, as defined in Section 3.1.

3.3 System Security Categorization

In accordance with NIST, FISMA, and OMB guidance (specifically NIST SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories," issued August 2008, and Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," issued February 2004), the purpose of the system security categorization (SecCat) is to clearly define the system's authorization boundary, users, architecture, and interfaces, and to ensure that the information and the information system are properly categorized in accordance with applicable Federal laws, Executive orders, directives, policies, regulations, standards, and guidance. The system owner must ensure that the relevant information owners and the system staff review the SecCat at least annually to ensure that all information types are properly identified and any changes to the authorization boundary are documented. All SecCats must be provided to CSO at the required frequency, as defined in Section 3.1.

3.4 Privacy Threshold Analysis/Privacy Impact Assessment Updates

The Privacy Act requires a privacy impact assessment (PIA). A privacy threshold analysis (PTA) is used to determine whether a PIA is needed. A system is not required to have a PIA if it does not collect, maintain, or disseminate information about individuals. If a PIA is not required, the system should have a PTA on file documenting this determination. The PTA template can be found at ADAMS Accession No. ML091970114. If the PTA determines that the system processes information about individuals (including members of the public), a PIA must be performed. The PIA assists in identifying and analyzing how personally identifiable information (PII) is processed within a system to ensure the following:

- PII handling conforms to applicable legal, regulatory, and policy requirements for privacy.
- The PIA addresses the risks and effects of collecting, maintaining, and disseminating PII in a system.
- The PIA examines and evaluates protections and alternative processes for handling PII to mitigate potential privacy risks.

The outcome of this process is a PIA document that provides the results of the assessment and is signed by the Privacy Officer. Comprehensive and accurate PIAs are required to identify all privacy risks and methods to mitigate the risks. The PIA template is at ML050460335. To ensure proper protection of the agency's PII, the PTA and PIA must be reviewed and updated at the frequency defined in Section 3.1.

3.5 Periodic Reviews and Risk Management Reporting

CSO conducts periodic and ongoing cybersecurity reviews of offices, regions, and contractor sites and their systems to provide senior officials with an agencywide view of the NRC's cybersecurity risk posture. System owners and the NRC AO are periodically briefed on cybersecurity metrics, continuous monitoring progress, and identified risks. This information is reflected in the CRDB, which, in turn, provides executives and their staff with the status of the security posture of their respective offices, regions, and systems. Cybersecurity risk management activities are not only required by FISMA and the OMB but also significantly underpin the NRC's ability to identify, manage, and minimize risk to the agency mission. Office Directors and Regional Administrators must ensure that any system-specific findings from cybersecurity control assessments, periodic scanning, configuration checks, OIG audits, and other testing are incorporated into their respective system POA&Ms, in accordance with CSO-PROS-2016, and, if appropriate, brought to the attention of the NRC AO.