Cybersecurity Risk Management Activities Instructions
Fiscal Year 2018

On December 18, 2014, to update the Federal Information Security Management Act of 2002, President 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 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 Office of the Chief Information Officer (OCIO)/Information Security Planning and Oversight Branch (ISPOB) to identify and maintain the agency's information security program, with oversight provided by the Chief Information Security Officer (CISO).

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 information security policies, procedures, and practices of the agency
- security awareness training
- procedures for detecting, reporting, and responding to security incidents
- periodic reporting requirements

In addition, the NRC must provide procedures for detecting, reporting, and responding to security incidents, including notification of Congress not later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred and, within a reasonable time thereafter, submit additional information regarding the incident, including a summary report. The NRC must also submit annual reports on the adequacy and effectiveness of its information security policies, procedures, and practices to designated agency officials and congressional committees.

An effective risk management program and compliance with FISMA requires 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 risk management program and related cyber risk management activities at both the agency and individual system levels.

At the agency level, continuous monitoring guidance, periodic reviews, cybersecurity training requirements, and the Cybersecurity Risk Dashboard[1] (CRDB) ensure that Office Directors and Regional Administrators are effectively managing cyber risk. At the system level, the System Owner implements continuous monitoring plans that address existing cyber risk management requirements to monitor changes to the system and cybersecurity controls to ensure the system's security posture is not degraded.

The Office of the Inspector General (OIG) has performed several audits and found that some required cybersecurity activities were either not performed or were delayed. In addition, the NRC was the subject of several Government Accountability Office audits that also found that it failed to perform required cybersecurity activities. In fiscal year (FY) 2018, it is expected that the U.S. Department of Homeland Security (DHS) continuous diagnostics and mitigation tools will be fully implemented to provide a continuous view into the NRC infrastructure configuration and vulnerability mitigation compliance.

1 GENERAL REQUIREMENTS

Beginning in FY 2018, it is expected that system security documents associated with the agency's internal cybersecurity program will be placed into a FISMA repository located in the Agencywide Documents Access and Management System (ADAMS). The purpose of this repository is to streamline the current document submission requirements (outlined below), thus reducing the burden on the System Owner's staff and decreasing the resources required to comply with annual Office of Management and Budget (OMB) and OIG FISMA audit requirements.

Until the agency approves, communicates, and distributes this new process, all FISMA-required continuous monitoring security artifact submissions must continue to be sent to the CISO@nrc.gov e-mail address using an ADAMS accession number (ML number). In the first sentence, the e-mail should state that it is provided as a cybersecurity continuous monitoring submission to give appropriate routing to the ISPOB. "Viewer" access level rights must be extended to groups "OCIO-GEMSD-ISPOB-Rev CTR," "OCIO-GEMSD-ISPOB-Rev Group," and "OIG-FISMA Audit," for all documents uploaded to ADAMS (documents containing security-related information should not be profiled to include all NRC users). If the information relates to a classified or Safeguards Information system, the e-mail should provide a reference pointing the recipient to the specific location of the required information (classified and Safeguards Information material are prohibited in ADAMS).

To promote good security practices and the best possible security posture, please complete FISMA-required continuous monitoring security artifacts by their respective due dates and submit them within 10 working days of completion. This will ensure effective communication of the most accurate information and achieve full credit during annual OIG FISMA reviews. Information System Security Officers (ISSOs) should coordinate with their ISPOB point of contact to ensure the data are accurate and current on the CRDB. The dashboard will reflect incomplete or late submissions, which may adversely affect system and office Cybersecurity Performance Index scores reported to Office Directors, Regional Administrators, the Chief Information Officer (CIO), and the Executive Director for Operations.

[1] See http://fusion.nrc.gov/OCIO/team/CSO/Cyber%20Risk%20Dashboard/Pilot/CRDB.html.

Office Directors, Regional Administrators, System Owners, or their representatives should engage (as necessary) ISPOB and the NRC Configuration Control Board (CCB) staff at the start of any initiative to develop, modernize, or enhance an information technology system. By engaging early, ISPOB and CCB staff and the project team will be able to discuss requirements and options and address any documentation and process questions, thereby minimizing schedule delays and cost. The ISPOB periodically reviews required cybersecurity activities with System Owners' staff and updates the agency's CRDB. The System Owner (or approved designee) has the responsibility to submit to ISPOB information that changes the status of these activities as tracked in the CRDB. The data contained in the CRDB are periodically reported to the CISO, the CIO, Office Directors, 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, including a cybersecurity review.

Section 2 of this document provides instructions to assist Office Directors and Regional Administrators in completing requirements for cybersecurity role identification and required role-based training.

Section 3 of this document assists the System Owner and provides instructions for completing the cyber risk management activities effectively. These tasks include the following:

- Laptop and Standalone Personal Computer Authorization
- Continuous Monitoring
- System Cybersecurity Assessment (SCA)
- System Security Categorization (SecCat)
- privacy threshold analysis (PTA)/privacy impact assessment (PIA) updates
- periodic reviews and risk management reporting

2 INSTRUCTIONS FOR OFFICE DIRECTORS AND REGIONAL ADMINISTRATORS

OMB Circular A-130, "Managing Information as a Strategic Resource," and FISMA require agencies to ensure 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 Training

Office Directors and Regional Administrators must ensure all staff and contractors complete the annual computer security awareness course.

2.2 Cybersecurity Role Identification and Required Role-Based Training

FISMA requires that all personnel with significant cybersecurity responsibilities be appropriately identified and trained. The NRC significant cybersecurity role definitions are available at: http://fusion.nrc.gov/OCIO/team/CSO/Training_And_Awareness. Effective June 14, 2004, the Office of Personnel Management (OPM) required agencies to develop a cybersecurity training plan for training 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," and SP 800-50, "Building an Information Technology Security Awareness and Training Program." OPM also encourages training to reflect the NIST National Initiative for Cybersecurity Education, located at https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity. The NRC cybersecurity training plan is located at http://fusion.nrc.gov/OCIO/team/CSO/Training_And_Awareness. The current training plan will be transitioning to include the Cybersecurity Workforce Development Plan in the near future. Office Directors and Regional Administrators must ensure that ISPOB and the Office of the Chief Human Capital Officer (OCHCO) 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 executives and must take role-based training for executives. The current list of individuals assigned to significant cybersecurity roles can be found at http://fusion.nrc.gov/OCIO/team/CSO/CyberRiskDashboard. A list of courses available in iLearn to assist with role-based training requirements can be requested by emailing CybersecurityTraining.Resource@nrc.gov. ISPOB is working with OCHCO to have cybersecurity roles identified, along with required curricula within iLearn.

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 ISPOB via a memorandum using CSO-TEMP-0002, "Office Information System Security Officer (ISSO) Appointment Letter." Additional information about the ISSO forum can be found at http://fusion.nrc.gov/OCIO/team/CSO/Training_And_Awareness, or by emailing CybersecurityTraining.Resource@nrc.gov. Offices may decide to have a single individual represent multiple offices. If this is the case, the appointment memorandum should so indicate. ISSO forum meetings provide the mechanism for ISSOs to learn 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 a primary and alternate system ISSO as their security representatives for the system via a memorandum using CSO-TEMP-0001, "System Information System Security Officer (ISSO) Appointment Memo Template."

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

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

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

(3) 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

Systems include those operated by or on behalf of the NRC, including all systems operated and maintained by contractors, all cloud-based systems, FedRAMP systems, and all other non-NRC Federal agency systems used by the NRC. All system weaknesses must be documented and managed through monthly updates in the system POA&M, and the POA&M must reflect a realistic plan to mitigate the weakness. CSO-PROS-2016, "Plan of Action and Milestones Process," contains instructions on POA&M creation and maintenance.

Contract vehicles are available through ISPOB to support the completion of cyber risk management requirements. Please refer to your office's contracting officer's representative for cybersecurity program support services for assistance with cost estimates for continuous monitoring activities.

All systems hardware, operating systems, and applications must meet cybersecurity policy and standards, including configuration standards. This also applies to laptops and standalone computers. Cybersecurity standards requirements can be found on the cybersecurity standards Web site at http://www.internal.nrc.gov/CSO/standards.html. To minimize resources, reduce costs, and streamline implementation, the NRC will no longer customize externally provided security configuration standards. If an NRC-specific standard does not already exist, the system must be configured in accordance with Defense Information Systems Agency (DISA) standards, checklists, and guidance. In the absence of both NRC standards and DISA requirements, the following must be used (in this order): Center for Internet Security benchmarks, vendor-provided guidance, and industry best practices. As these organizations determine new configuration standards, the NRC environment will require them within 6 months of issuance. Awareness and adherence to these standards yield fewer weaknesses that have to be added to a POA&M and help minimize the cost and risk associated with findings.

As system cybersecurity artifacts are developed for system authorization requests, or updated and submitted to ISPOB in support of the continuous monitoring activities outlined below, System Owners must ensure that these artifacts meet the minimum requirements prescribed by CSO-PROC-2104, "System Artifact Examination Procedure." 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.

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

3.1 Laptop and Standalone Personal Computer Authorization

All NRC laptops and standalone personal computers must belong to a system boundary (which may contain one or more devices), and that system must be authorized to operate. Each office and region can have up to one of each of the following types of laptop/standalone personal computer systems:

- general laptop/standalone personal computer system
- safeguards information laptop/standalone personal computer system
- classified information laptop/standalone personal computer system

System Owners must obtain system authorization using the following:

(1) CSO-TEMP-3001, General Laptop/Standalone Desktop System Request for Authorization Memorandum Template

(2) CSO-TEMP-3003, Safeguards Information Laptop/Standalone Desktop System Request for Authorization Memorandum Template

(3) CSO-TEMP-3005, Classified Information Laptop/Standalone Desktop System Request for Authorization Memorandum Template

To reduce costs, simplify security, and ensure timely and efficient helpdesk support, System Owners are encouraged to use laptops and workstations configured and managed by OCIO to the extent practical, instead of maintaining and securing their own. To realize these benefits and ensure the above requirements are satisfied, offices shall coordinate with OCIO to ensure that any IT devices purchased are configured, maintained, and secured to meet NRC requirements.

3.2 Continuous Monitoring

Information security continuous monitoring (ISCM) activities 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 ISCM is the constant, near real-time detection and management of risk.

Continuous monitoring requirements apply to the NRC's established systems (including contractor systems), cloud-based systems, FedRAMP systems, and other external Federal agency systems used by the NRC.

System Owners must ensure that all systems are authorized by the NRC Authorizing Official and follow CSO-PROS-1323, "Information Security Continuous Monitoring Process" (http://www.internal.nrc.gov/CSO/processes.html). The NRC provided CSO-PROS-1323 to OMB as required to outline the agency's continuous monitoring process and to capture requirements from NIST SP-800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," as well as OMB Circular A-130, and provides clear instructions for maintaining an effective risk management program for systems authorized by the NRC Authorizing Official. 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 ease of reference, NRC-defined continuous monitoring frequencies and timeframes are identified at

http://fusion.nrc.gov/OCIO/team/CSO/isd/Cyber%20Security%20Issuances/03_CKLT_PROC_PROS_TEMP/03_CSO-PROS-1323_Frequencies_V2.0%20-%20ML16307A338.pdf.

3.3 System Cybersecurity Assessment

As prescribed by NIST, OMB, and FISMA requirements, the purpose of the SCA is to determine the extent to which cybersecurity controls are implemented, operate as intended, and produce 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 the Information System Owner, common control provider, and Authorizing Official 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.

3.4 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," and Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," the purpose of the SecCat is to provide a clear definition of the system's authorization boundary, users, architecture, and interfaces, and to ensure proper categorization of the information and the information system 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 proper identification of all information types and ensure the documentation of any changes to the authorization boundary. In 2017, the NRC completed an agencywide effort to define risk tolerance and sensitivity levels at the agency level and to streamline the development and maintenance of all NRC SecCats. All SecCats must be provided to ISPOB at the required frequency as in Section 3.2 above.

3.5 Privacy Threshold Analysis/Privacy Impact Assessment Updates

The Privacy Act requires a privacy impact analysis. A PTA is used to determine whether a PIA is needed. Some systems will not require a PIA if the system will 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 in 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 about privacy.
- It addresses the risks and effects of collecting, maintaining, and disseminating PII in a system.

- It 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 Act Officer. Comprehensive and accurate PIAs are required to identify all privacy risks and methods to mitigate the risks. The PIA template is at ADAMS Accession No. ML050460335.

To ensure proper protection of the agency's PII, the PTA/PIA must be reviewed at least annually and provided to ISPOB within 20 working days of any change.

3.6 Periodic Reviews and Risk Management Reporting

ISPOB conducts periodic and ongoing cybersecurity reviews of offices, regions, contractor sites, and their systems to provide senior officials with an agencywide view of the NRC's cybersecurity risk posture. Various cybersecurity metrics, continuous monitoring progress, and identified risks are periodically briefed to System Owners and the NRC Authorizing Official. This information is reflected on the CRDB, which, in turn, provides executives and their staff with 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 significantly underpin the ability of the NRC 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 and configuration checks, OIG audits, and other testing are incorporated into their respective system POA&Ms, in accordance with CSO-PROS-2016, and, if appropriate, are brought to the attention of the NRC Authorizing Official.