Cybersecurity Risk Management Activities Instructions
Fiscal Year 2016

On December 18, 2014, President Obama signed into law the "Federal Information Security Modernization Act of 2014" (FISMA), which serves to strengthen the security of computer networks and information systems by updating the Federal Information Security Management Act of 2002. 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 agency-wide information security program to provide security for information and support systems. The Nuclear Regulatory Commission (NRC) directorate designated to carry out these functions is the Office of the Chief Information Office (OCIO) / Information Security Directorate (ISD), headed by the Chief Information Security Officer.

FISMA requires that the NRC information security program include:

- periodic assessments of the risk and magnitude of potential harm;
- policies and procedures to cost-effectively reduce information security risks based on risk assessments;
- ensuring that information security is addressed throughout the life cycle of each agency information system;
- minimally 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 testing and evaluation of the effectiveness of policies, procedures, practices and procedures; and
- periodic reporting requirements.

In addition, NRC must provide the procedures for detecting, reporting, and responding to security incidents, including notification of Congress of any major incident not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred and, within a reasonable time thereafter, additional information regarding the incident, including a summary report. 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 risk management program and related cyber risk management activities are implemented at the agency as well as individual system levels.

At the agency level, the Cybersecurity Risk Dashboard[1] (CRDB), continuous monitoring guidance, periodic reviews, and cybersecurity training requirements are established to ensure 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.

In Fiscal Year (FY) 2014 and FY 2015, the Office of the Inspector General (OIG) found that some required cybersecurity activities were either not performed or were delayed. To avoid repeat findings and to minimize risk to NRC's mission, ISD and the Office of the Executive Director for Operations will ticket overdue cybersecurity requirements.

1 GENERAL REQUIREMENTS

All FISMA-required continuous monitoring submissions must be sent to the RidsOCIO Resource email using an Agencywide Documents Access and Management System (ADAMS) Accession Number (ML number) and be Official Agency Records (OAR). "Viewer" access level rights must be extended to groups "OCIO-ISD Review Contractor," "OCIO-ISD Review 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). To ensure effective communication of the most accurate information, and to ensure full credit during annual OIG FISMA reviews, please ensure FISMA-required continuous monitoring security artifacts are completed by their required due date and submitted within 10 working days of completion. Information System Security Officers (ISSOs) should coordinate with their ISD Point of Contact (POC) to ensure Cybersecurity Risk Dashboard data is accurate and current. Incomplete or late submissions will be reflected on the cybersecurity dashboard and may adversely affect system and office Cybersecurity Performance Index scores reported to Office Directors, Regional Administrators and the DAA.

Office Directors, Regional Administrators, or their representatives should engage the ISD at the start of any initiative to develop, modernize or enhance an information technology system. By engaging early, ISD staff and the project team will be able to discuss requirements, options, and address any documentation and process questions, thereby minimizing schedule delays and cost.

The ISD periodically reviews required cybersecurity activities with System Owner staff and updates the agency's CRDB. It is the responsibility of the System Owner to submit to ISD information that changes the status of these activities as tracked in the CRDB. The data contained in the CRDB is periodically reported to the Major Information Technology Investment DAA (as designated in ML15302A197), Office Directors, the OIG, and System Owners as appropriate.

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 is intended to assist the System Owner and provide instructions for completing the cyber risk management activities effectively. These tasks include the following:

[1] http://fusion.nrc.gov/ois/team/isd/FCO/Cyber%20Risk%20Dashboard/Pilot/CRDB.html

- Laptop and Standalone Personal Computer Authorization,
- Continuous Monitoring,
- System Cybersecurity Assessment,
- System Security Categorization,
- Privacy Threshold Analysis / Privacy Impact Assessment Updates, and
- Periodic Reviews and Risk Management Reporting

2 INSTRUCTIONS FOR OFFICE DIRECTORS AND REGIONAL ADMINISTRATORS

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. 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://www.internal.nrc.gov/CSO/Cybersecurity-Roles.html. 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." The NRC cybersecurity training plan is located at: http://www.internal.nrc.gov/CSO/CyberSecTrngEd.html. The current training plan will be transitioning to the Cybersecurity Workforce Development Plan in the near future.

Office Directors and Regional Administrators must ensure that ISD 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 to within 20 business days of any change in roles. 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://www.internal.nrc.gov/CSO/CyberSecTrngEd.html. A list of courses available in iLearn to assist with role-based training requirements can be found at: http://www.internal.nrc.gov/CSO/CyberSecTrngEd.html.

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 ISD via memorandum using CSO-TEMP-0002, "Office Information System Security Officer (ISSO) Appointment Letter." 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 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, system owners must appoint a primary and alternate system ISSO as their security representatives for the system via memorandum using CSO-TEMP-0001, "System Information System Security Officer (ISSO) Appointment Memorandum Template."

Office Directors and Regional Administrators must ensure their:

1. Office ISSOs participate in the ISSO forum meetings, bi-annual all-ISSO meetings, and cybersecurity seminars.
2. System ISSOs participate in the bi-annual all-ISSO meetings and cybersecurity seminars.
3. Staff with significant cybersecurity responsibilities complete the mandatory security-related training detailed in the NRC cybersecurity training plan (to be replaced by the Cybersecurity Workforce Development Plan upon issuance).

3 INSTRUCTIONS FOR SYSTEM OWNERS

Systems include those operated by or on behalf of 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 NRC.

Contract vehicles are available through ISD to support the completion of cyber risk management requirements. Please refer to your Office Cyber Security Program Support Services (CSPSS) Contracting Officer's Representative (COR) 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 website at http://www.internal.nrc.gov/CSO/standards.html. In order 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 Center for Internet Security (CIS) benchmarks must be used. As new configuration standards are issued by these organizations, they will be required within the NRC environment within six months of issuance.

As system cybersecurity artifacts are developed for system authorization requests, or updated and/or submitted to ISD 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, operating as intended, producing 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 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
1. CSO-TEMP-3003, Safeguards Information Laptop/Standalone Desktop System Request for Authorization Memorandum Template
2. CSO-TEMP-3005, Classified Information Laptop/Standalone Desktop System Request for Authorization Memorandum Template

To save cost, simplify security and ensure timely and efficient helpdesk support, System Owners are encouraged to use seat-managed laptops distributed and maintained by the OCIO to the extent practical, instead of maintaining their own laptops. OCIO is the System Owner for the seat-managed laptops and ensures the above requirements are satisfied.

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 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.

Continuous monitoring requirements apply to NRC established systems (including contractor systems), cloud-based systems, and other external federal agency systems used by NRC.

System owners must ensure that all systems are authorized by the NRC DAA and follow CSO-PROS-1323, "Information Security Continuous Monitoring Process" (ML14091A703). CSO-PROS-1323 has been provided to OMB as required to outline the NRC continuous monitoring process and captures requirements from NIST SP-800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," as well as OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, and provides clear instructions for maintaining an effective risk management program for systems authorized by the NRC DAA. This requirement applies to NRC owned systems, NRC contractor owned or operated systems, and all non-NRC federally owned or operated systems which store

or process NRC data. For ease of reference, NRC-defined continuous monitoring frequencies and timeframes are identified at http://fusion.nrc.gov/ois/team/isd/Cyber%20Security%20Issuances/Processes/CSO-PROS-1323_Frequencies.pdf.

3.3 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 (documented in a SCA-report) provide insight into the current security state of a system, and an assessment of risk is performed that reflects the results of various continuous monitoring and other assessment and review activities. The SCA contains a list of recommended corrective actions for weaknesses or deficiencies identified in the security controls. The SCA must be reviewed at least quarterly by the System Owner (or designee) and updated as new weaknesses are identified, existing risks are mitigated, and as System Owner assessments of new/known risks evolve. Updates to the SCA support near real-time risk management and help to ensure the information system owner, common control provider, and DAA maintain appropriate awareness with regard to security control effectiveness. The overall effectiveness of the security controls directly affects the ultimate security state of the information system and decisions regarding explicit acceptance of risk.

3.4 System Security Categorization

As per 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 (FIPS) 199, “Standards for Security Categorization of Federal Information and Information Systems” the purpose of the Security Categorization (SecCat) is to provide 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 the SecCat is reviewed by the relevant Information Owners and the system staff at least annually to ensure proper identification of all information types and ensure any changes to the authorization boundary have been documented. In FY 2016, an agency-wide effort to define risk tolerance and sensitivity levels is intended to streamline the development and maintenance of all NRC SecCats. Until that time, the SecCat must be provided to ISD per the required frequency as in section 3.2 above.

3.5 Privacy Threshold Analysis / Privacy Impact Assessment Updates

Privacy impact analysis is required by the Privacy Act. A Privacy Threshold Analysis (PTA) is used to determine whether a Privacy Impact Assessment (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 (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 PII is processed within a system to ensure the following:

- Personally Identifiable Information (PII) handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Risks and effects of collecting, maintaining, and disseminating PII in a system are addressed; and
- Protections and alternative processes are examined and evaluated for handling PII to mitigate potential privacy risks.

The outcome of the PIA process is a document that provides the results of the assessment and is signed by the Privacy Act Officer. Comprehensive and accurate PIAs are required to ensure that all privacy risks and methods to mitigate the risks are identified. The PIA template can be found in ADAMS (ML050460335).

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

3.6 Periodic Reviews and Risk Management Reporting

Periodic and ongoing cybersecurity reviews of offices, regions, and their systems are conducted by ISD to provide senior officials with an NRC-wide view of the agency's cybersecurity risk posture. Various cybersecurity metrics, continuous monitoring progress, and identified risks are periodically briefed to System Owners and the NRC DAA. 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 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 security documentation (such as system security plans and plans of action and milestones) and, if appropriate, brought to the attention of the NRC DAA.