Cybersecurity Risk Management Activities Instructions
Fiscal Year 2015

An effective risk management program and compliance with the Federal Information Security Management Act (FISMA) requires the U.S. Nuclear Regulatory Commission (NRC) to continuously monitor system security posture, 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 and 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.

General Requirements

At the system level, continuous monitoring involves several key tasks: assessing security control effectiveness, responding to risks identified during assessments (including vulnerability scans and configuration checks of system components), maintaining system security artifacts, performing required tests, and reporting the security state of the system to designated organization officials. The security-related information obtained and reported during continuous monitoring informs NRC Designated Approving Authority (DAA) risk-based decision making.

Continuous monitoring tasks are performed concurrently by system security staff. For example, systems personnel respond to risks that were identified during periodic vulnerability scans, maintain information within the system POA&M, and maintain system artifacts on an ongoing basis. Special attention on POA&Ms is necessary, as they are a critical system owner responsibility. POA&M management will help your office monitor the progress of corrective actions relative to known weaknesses in security controls, and provides an accurate measure of security program effectiveness. Internal and independent assessments of the implementation of security controls are also conducted throughout the cycle.

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

Required security controls may also have many components, including enhancements. As a result, a single control may have different continuous monitoring requirements and frequencies associated with the different components. This is an example of security control tailoring, which is used by organizations to achieve cost-effective, risk-based security that supports organizational mission/business needs.

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

System Information System Security Officers (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.

Office Directors and Regional Administrators are also responsible for ensuring that staff and contractors who have significant system and cybersecurity responsibilities (e.g., system administrators and ISSOs) complete the necessary and required role-based training. For these individuals, cybersecurity is an inherent part of their job.

Reporting Requirements

Office Directors, Regional Administrators, and System Owners must notify the Computer Security Office (CSO) of activities performed during the year to meet the annual cyber risk management requirements to ensure that these activities are properly credited. Instructions for notifying CSO of completed activities and submission of required deliverables are provided in this document. Where the provision of required documentation to CSO is specified in section A below, all submissions must be forwarded to the RidsCsoMailCenter Resource email. Documents must be submitted by using the Agencywide Documents Access and Management System (ADAMS) Accession Number (ML number) and be Official Agency Records (OAR). "View Content" and "View Props" access rights must be extended to groups "CSO Review Contractor", "CSO Review Group", and "OIG [Office of the Inspector General] -FISMA Audit" for all documents uploaded to ADAMS.

All testing activities (e.g., Contingency Plan Testing and Periodic Security Control Tests) must be completed and the final test reports dated *within the required time frame (e.g., one year) of the previous test report* date. The agency's CRDB may be referenced for the status and current due dates (or most recent known completion date) of each required activity. These activities are subject to periodic Independent Verification and Validation (IV&V) reviews by CSO.

In FY14, the OIG found that some continuous monitoring activities were either not performed or delayed. To avoid repeat findings and to minimize risk to NRC's mission, CSO, and, as necessary, OEDO will create a Rids ticket for the completion of any requirement specified in section A that becomes overdue in FY15 or is already overdue.

All systems' hardware, operating systems, and applications must meet cybersecurity policy and standards, including configuration standards. This also applies to laptops and standalone computers (for additional details see section B.3, Laptop and Standalone Personal Computer Authorization). Cybersecurity standards requirements can be found on CSO's Cybersecurity Standards website at http://www.internal.nrc.gov/CSO/standards.html. If a CSO specific standard does not exist, the system must be configured in accordance with Defense Information Systems Agency (DISA) standards, checklists, and guidance. In the absence of both CSO standards and DISA requirements, the Center for Internet Security (CIS) benchmarks must be used.

As system cybersecurity artifacts are developed for system authorization requests or updated 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). CSO staff and independent assessors must also use this procedure to evaluate the acceptability of the artifacts.

Office Directors and Regional Administrators must engage the CSO at the start of any initiative to develop a new information technology system or to modernize or enhance an existing system. System security is a critical function and should be addressed at the onset of any information technology project. By engaging early, CSO staff and the project team will be able to discuss requirements, options, and address any documentation and process questions.

Section A of this document is intended to assist the System Owner and provide instructions for completing the cyber risk management activities effectively, according to FISMA requirements, Federal Information Processing Standard (FIPS) Publication 200 Minimum Security Requirements for Federal Information and Information Systems, and the general DAA conditions required of the systems' Authorization to Operate (ATO). These tasks include the following:

A.1. Contingency Plan (CP) Testing
A.2. Periodic System Cybersecurity Assessment (PSCA)
A.3. Security-Related Documentation Updates
A.4. Vulnerability Scanning and Configuration Compliance
A.5. POA&M Updates
A.6. Compliance with Requirements for Systems Authorized by Other Agencies

The CSO periodically reviews the above and provides updates on the completion of activities. Results of these reviews are used to update the agency's CRDB. It is the responsibility of the System Owner to notify the CSO upon any change to 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 ML12083A054), Office Directors, and System Owners as applicable.

Section B of this document provides instructions to assist Office Directors and Regional Administrators in completing requirements for the following:

B.1. Cybersecurity Role Identification
B.2. Cybersecurity Awareness Course and Role-Based Cybersecurity Training
B.3. Laptop and Standalone Personal Computer Authorization
B.4. Periodic Reviews and Risk Management Status Reports

Contract vehicles are available through CSO 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 annual continuous monitoring activities.

A. Instructions for System Owners

A.1. Contingency Plan Testing

CP testing validates recovery capabilities to improve plan effectiveness and overall organization preparedness to execute the plan. This provides assurance that the plan remains current with system and organizational changes. CP test report dates must not exceed one year from the date of the prior CP test report. CP test due dates are specified in the CRDB. To ensure the Office of Information Services (OIS) has resources available when needed, the System Owner should schedule CP testing with OIS at least 90 calendar days in advance of the test, if OIS coordination is required.

The requirements in this section apply to systems owned by the NRC and systems operated on behalf of the NRC by contractors. The following list identifies major milestones to incorporate into the CP testing schedule:

1. Conduct and document a Business Impact Analysis (BIA) or update the existing BIA. The BIA must be reviewed, updated, declared an official record and provided to CSO within 20 business days of changes and at least annually, dated less than 1 year after the date of the last report.
2. Develop a Contingency Test Plan for testing the CP. The Contingency Test Plan must be reviewed, updated, declared an official record and provided to CSO within 20 business days of changes and at least annually, dated less than 1 year after the date of the last test plan.
3. Conduct annual CP training for staff with contingency planning roles and responsibilities.
4. Coordinate testing with affected organizations.
5. Execute CP testing according to the Contingency Test Plan.
6. Develop a Contingency Test Report to document the results of testing. The Contingency Test Report must be reviewed, updated, declared an official record and provided to CSO within 20 business days of changes and at least annually, dated less than 1 year after the date of the last report.
7. Ensure that weaknesses identified through CP Testing are incorporated into the system's POA&M in accordance with CSO-PROS-2016, "Plan of Action and Milestones Process."
8. Ensure that the CP test information is entered into relevant POA&M items in accordance with CSO-PROS-2016.
9. Update the CP to reflect the results of CP testing and lessons learned. The CP must be reviewed, updated, declared an official record and provided to CSO within 60 calendar days of completion of testing and delivery of the CP Test Report, and dated less than 1 year after the date of the last test report.

For additional information please see National Institute of Standards and Technology (NIST) Special Publication (SP) SP 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations,* NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information System*s, and CSO-STD-0020, *Organization Defined Values for System Security Controls* (http://www.internal.nrc.gov/CSO/standards.html).

A.2 Periodic System Cybersecurity Assessment

System Owners must ensure that an independent System Cybersecurity Assessment (SCA) is conducted periodically on the system (and at least annually) by an independent assessment team to affirm the effectiveness of security controls. The frequency of these assessments may

vary based upon the sensitivity of the system (for details, see CSO-STD-0020, Organization Defined Values for System Security Controls, control CA-2). The CSO annually identifies a set of core security controls based upon current risks that must be assessed during independent periodic testing. This requirement provides the necessary assurance that federally mandated and NRC defined security controls are being implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Testing completion dates must not exceed one year from the date of the last SCA report. SCA due dates are specified in the CRDB. The independent assessment team works with the System Owner to:

1. Develop a security controls testing schedule.
2. Select controls that must be tested. These controls include CSO-defined core controls, controls associated with POA&M weaknesses that were closed within the past year, compensating controls and/or mitigating factors related to approved Deviation Requests (DRs), and any other additional controls selected by CSO or the System Owner.
3. Develop and submit to CSO for review prior to testing, a test plan using the CSO-TEMP-2027, Security Control Test Plan template for the system.
4. Perform a comprehensive security assessment of the selected security controls using the test plan.
5. Document the results of the security controls testing in a SCA report. This report must be must be reviewed, updated, declared an official record, and provided to CSO within 20 business days of the report date.
6. Ensure that weaknesses identified through SCAs are incorporated into the system's POA&M in accordance with CSO-PROS-2016.
7. Ensure that the SCA test completion information is entered into relevant POA&M items in accordance with CSO-PROS-2016.

A.3 Security-Related Documentation Updates

The update of system security documentation, particularly the System Security Plan (SSP), Security Risk Assessment (SRA), POA&M, Security Categorization Report (SecCat) and the Privacy Threshold Analysis (PTA) / Privacy Impact Assessment (PIA), is an essential component of cyber risk management. Maintaining these documents ensures that the system security posture is accurately documented as changes are made, and/or as threats, vulnerabilities, technologies, and business requirements and processes evolve. The following sections describe the updates required for critical security documents and their associated frequency.

A.3.a. SSP Updates

The results of all system security-related activities are documented in the SSP. The SSP reflects any modifications to security controls based on risk assessment and/or mitigation activities carried out by the information system owner or common control provider. To maintain an accurate understanding of the security posture of the system and to support risk management activities, the SSP must be reviewed at least quarterly and updated to address changes arising from or related to the items listed below:

1. Weaknesses or deficiencies discovered in currently deployed security controls after a system breach.
2. Modifications to security controls (or control status) based on risk mitigation activities.
3. New or modified system interconnections.
4. Changes to hardware, software, and system boundary, including newly hosted applications.
5. Continuous monitoring activities (e.g., security control assessments, periodic scans).
6. System-specific conditions as specified by the DAA as part of an authorization decision or other periodic risk management review.
7. Other security-related activities (e.g., Security Impact Assessments/System Change Authorizations, Security Assessment Reports, SCAs, CP testing, Inspector General findings, IV&V Reports).

The SSP must be reviewed, updated and declared an official record within 20 business days of changes and a current version provided to CSO quarterly, by the 15th day of November, February, May, and August. Any supporting documentation referenced in the SSP (e.g., configuration management plan, operation/administrator guides, policy/procedure documents) or affected by system changes must also be reviewed quarterly and updated accordingly. Even if there are no changes in a given quarter, an entry should be made in the SSP change log stating "SSP Quarterly Update" and dated within the appropriate quarter.

The System Owner may choose to maintain an errata sheet in the SSP to track ongoing system changes prior to each quarterly review and update. Once the quarterly review and update has been completed, the errata sheet can be discarded.

Additionally, the recent OIG Independent Evaluation of NRC's FISMA Implementation for FY14 found that NRC SSPs were not updated to reflect changes to NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, with the issuance of Revision 4 in April 2013. So that the NRC can ensure the effectiveness of information security controls, all system security plans must be updated to be reflect NIST SP-800-53 Revision 4 by September 30, 2015.

A.3.b. SRA Updates

The purpose of the SRA is to assess risk and reflect the results of various continuous monitoring and other assessment and review activities. The SRA contains a list of recommended corrective actions for weaknesses or deficiencies identified in the security controls. The SRA 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 SRA 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.

A.3.c. Security Categorization Updates

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 SecCat is reviewed by the System Owner at least annually to ensure proper identification of all information types and ensure any changes to the authorization boundary have been documented. The SecCat must be provided to CSO at least annually, or upon change to the system boundary or information used by the system. Upon any modification, a SecCat approval request (CSO-TEMP-2001) must be provided to CSO within 20 business days.

A.3.d 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:

- 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 CSO with 20 business days of any change.

A.3.e Other Updates

Supporting documentation (e.g., configuration management plan, documented configurations in recovery, rebuild, or other operational support procedures, inventory, system architecture document, design document, etc.) must be updated to reflect changes to the system and/or organization within 60 calendar days of change and placed in ADAMS (upon request) for CSO and/or OIG review. Changes must be tracked and approved as part of a formal change control process. Agency configuration management tools are available through the Office of Information Services.

A.4. Vulnerability Scanning and Configuration Compliance

Patching is the process of applying software designed to fix security issues and vulnerabilities and improve usability or performance. Vulnerability scanning is conducted to identify

vulnerabilities in the system and help to identify patches that need to be applied. Periodic patching, vulnerability scanning, and configuration compliance ("hardening") checks support cyber risk management by using automated tools to facilitate near real-time risk management for information systems.

System Owners must scan, patch and check the configuration compliance of their systems with the rigor and frequency appropriate for the system sensitivity level. System patching, vulnerability scans, and findings remediation must be performed and documented in accordance with CSO-STD-0020 and CSO-PROS-1401, "Periodic System Scanning Process," and provided to CSO within 20 business days of the respective report date.

Table 1: Vulnerability Scanning and Hardening Check Activities

Required Frequencies (per CSO-STD-0020)						
Activity	**Low Systems**	**Moderate Systems**	**High Systems**	**General Laptops**	**SGI Laptops**	**Classified Laptops**
Vulnerability Scans	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly
Hardening Checks	Quarterly	Quarterly	Quarterly	Annually	Annually	Annually
Wireless Scanning (Systems that contain a wireless component)	Quarterly	Quarterly	Quarterly	Not Applicable (N/A)	N/A	N/A

System Owners must complete the following to continuously detect and resolve vulnerabilities in their systems:

1. Track patch and vulnerability management through a formal change control process.
2. Establish a schedule for patching and system vulnerability scanning that is aligned to resolve vulnerabilities and verify fixes. Conducting patching prior to scanning will reduce the number of vulnerabilities in the scan results, thereby reducing the number of vulnerabilities to be resolved and tracked in the POA&M.
3. Ensure routine scans and security checks are conducted in a timely fashion.
4. Document the results of vulnerability assessment testing in accordance with CSO-PROS-1401.
5. Ensure that weaknesses identified through testing are incorporated into the system's POA&M in accordance with CSO-PROS-2016.

A.5 POA&M Updates

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

Annual reviews by the OIG have documented several recurring shortcomings within agency POA&Ms. In order to improve agency POA&M performance, system staff should focus attention upon the following key Office of Management and Budget (OMB) and NRC requirements when updating system POA&Ms:

1. Scheduled completion dates must not be changed.
2. All weaknesses should have a scheduled completion date.
3. All weaknesses should identify the source of the weakness.
4. All closed weaknesses should have an actual completion date.
5. Weakness must be reported as delayed once the scheduled completion date has passed.

The following list summarizes the major steps (detailed in CSO-PROS-2016) for developing, updating, and maintaining a POA&M:

1. Identify weaknesses using results of recent testing and continuous monitoring activities (e.g., Security Assessment Report, SCA, CP testing, vulnerability scanning, IG findings, system-specific ATO conditions, etc.).
2. Add these weaknesses to the POA&M in accordance with timeframes specified in the POA&M process and prioritize them to ensure the most critical security weaknesses (having the greatest potential impact to the organization's mission) are addressed first. Generally, weaknesses assessed as "High" or "Moderate" risk should be mitigated before "Low" risk weaknesses.
3. All weaknesses must identify the source of the weakness. Once added, weakness identifiers and descriptions must not be changed.
4. Identify and document the mitigation method based on effectiveness and cost for each weakness in the POA&M.
5. Determine the resources required for the corrective actions along with associated estimated costs. Document the funding availability (Funded, Reallocated, or Unfunded) in the POA&M.
6. Assign, based on the results of the steps above, the estimated completion date for each of the weaknesses. Once assigned, the completion dates shall not be changed.
7. Report as "delayed" all weaknesses not completed by the estimated completion date.
8. Document milestones for each weakness. Include the completion date or dates for resolving the milestones. Milestone completion dates may change (whereas, weakness completion dates may not be changed). If the milestone completion date is changed, document the reasons for the changes in the "Changes to Milestones" field.
9. Close weaknesses only if they have been fully mitigated, tested, and documented. While the testing demonstrates that the vulnerability or control weakness has been adequately addressed, clearly documenting the results is necessary for verification by an independent assessor or auditor.
10. Evidence of closure must be saved in ADAMS as an OAR and may consist of test results, resolution of Technical Change Request, an approved DR, etc. The evidence must be referenced with its ADAMS accession number in the "Changes to Milestones" field for the respective weakness.
11. Assign an actual completion date to all closed weaknesses.
12. Remove weaknesses only after they have been closed for more than one year.

All POA&M updates must be entered into the agency's information assurance tool before the quarterly snapshot dates (the 15th day of each November, February, May, and August). In order to assist System Owners in effectively managing IT system risks, POA&Ms are

periodically assessed to facilitate security improvements throughout the agency and to provide cybersecurity risk posture information to the NRC DAA.

Please refer to the POA&M Process for additional guidance on POA&M updates, submission, and evaluation. CSO is currently updating the process to more effectively achieve improved agency-wide cybersecurity. Notification of the update will be provided to all NRC Information System Security Officers (ISSO) upon completion.

A.6 Annual Requirements for Systems Authorized by Other Agencies

Some NRC organizations use systems owned and/or operated by other agencies. NRC organizations using systems owned and/or operated by other agencies (e.g., e-Government systems), must ensure that these systems also satisfy the annual requirements and maintain a valid ATO provided by the sponsoring agency. These systems must also be authorized for NRC use by the NRC DAA. For such systems, the applicable NRC Office Director must:

1. Verify that day-to-day security operations of the interconnected system(s) are carried out including periodic vulnerability assessment scanning, annual CP testing and periodic control testing.
2. Submit evidence of the execution of annual contingency plan testing and periodic security control testing to the CSO within one year and one month of the previous test report date.
3. Ensure that terms of any applicable Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA) are reviewed annually, carried out accordingly, and submitted to CSO within one year and one month of the previous document date.
4. Ensure that terms of any NRC approved Authority to Use (ATU) are reviewed within one year of the date of the ATU (and annually thereafter) and are carried out accordingly.
5. Ensure that the sponsoring agency maintains the system ATO in accordance with NIST Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems and provide the most recent sponsoring agency-issued ATO memorandum to CSO, ensuring that only fully authorized system are used by or on behalf of NRC.
6. Ensure that the system maintains its authorization granted by the NRC DAA, and is re-authorized by the NRC DAA upon any significant change that might give rise to additional/other risks within 30 calendar days of change implementation.
7. Notify the NRC DAA for non-major IT investments of an ATO expiration or termination, significant changes, unacceptable risks, or any change to the MOU/ISA at least 30 calendar days in advance of such events.
8. Ensure the system has a formal ATU granted by the NRC DAA for non-major IT investments before system use.

The CSO periodically reviews the status of these systems to ensure that each has a current authorization and that the requirements listed above are successfully completed. Results of these reviews are used to update the agency's CRDB. The data contained in the CRDB is periodically reported to the Major Information Technology Investment DAA, Office Directors, and System Owners as applicable.

B. Instructions for Office Directors and Regional Administrators

B.1. Cybersecurity Role Identification

FISMA requires that all personnel with significant cybersecurity responsibilities be appropriately identified. Effective June 14, 2004, the Office of Personnel Management (OPM) required agencies to identify employees with significant cybersecurity responsibilities and develop a cybersecurity training plan. The plan must include provisions for role-specific training as detailed NIST (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/training.html#Role-based. The current training plan will be transitioning to the Cybersecurity Workforce Development Plan in the near future.

Office Directors and Regional Administrators must maintain the 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 NRC significant cybersecurity role definitions are available at: http://www.internal.nrc.gov/CSO/Cybersecurity-Roles.html. The current list of assigned significant cybersecurity roles can be found at: http://www.internal.nrc.gov/CSO/training.html.

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

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

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

B.2. Cybersecurity Awareness Course and Role-Based Cybersecurity Training

OMB Circular A-130, Management of Federal Information Resources, and FISMA require agencies to ensure all individuals receive security awareness training and specialized training focused on their cybersecurity role and responsibilities. To ensure these requirements are met, Office Directors and Regional Administrators must ensure their:

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

The completion status for both cybersecurity awareness and role-based training can be found on the NRC Cybersecurity Risk Dashboard.

B.3 Laptop and Standalone Personal Computer Authorization

All NRC laptops and standalone personal computers must belong to a system, and that system must be authorized to operate. System owners must obtain system authorization using the following:

1. CSO-TEMP-3001, General Laptop/Standalone Desktop System Request for Authorization Memo Template
2. CSO-TEMP-3003, Safeguards Information Laptop/Standalone Desktop System Request for Authorization Memo Template
3. CSO-TEMP-3005, Classified Information Laptop/Standalone Desktop System Request for Authorization Memo Template

Note that System Owners are encouraged to use seat-managed laptops distributed and maintained by the OIS Operations Division to the extent practical, instead of maintaining their own laptops. OIS is the System Owner for the seat-managed laptops and ensures the above requirements are satisfied.

B.4 Periodic Reviews and Risk Management Status Reports

Periodic reviews of offices and regions and their systems are conducted by the CSO to provide senior officials with an NRC-wide view of the agency's cybersecurity posture. The results of these reviews are provided to the Deputy Executive Directors (DEDOs)/DAA and are reflected on the CRDB. The purpose of the periodic reviews is to provide System Owners and the NRC DAA with the status of the security posture of offices, regions, and systems and the progress made by each office and region in satisfying continuous monitoring requirements. These requirements are essential to support the overall cyber risk management activities of the NRC and the continued acceptance of any residual risk during ongoing operation.

Systems are evaluated to verify the timely completion of the risk management activities described in this document. Additionally, security artifacts are assessed to ensure accuracy and that security documentation requirements are being met (e.g., ISSO Appointment Letters, SIAs, DR, Privacy Impact Assessments, and MOU/ISAs, etc.).

Security documentation is also reviewed to ensure all identified risks/threats from various assessment tests, OIG audits, authorized and unauthorized system changes, and CSO IV&V assessments are identified and documented in the POA&M or an approved DR. The accuracy and completion of security documentation as related to contingency planning (BIAs, CPs, CP Test Reports, etc.) is also reviewed.

Office Directors and Regional Administrators must ensure that any system-specific findings from independent assessors, periodic IV&V reviews, or other sources of identified risk, are incorporated into the SSP, POA&M and SRA, and brought to the attention of the DAA in coordination with CSO.