U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 12.5	NRC CYBERSECURITY PROGRAM	DT-17-16
Volume 12:	Security	
Approved by:	David J. Nelson Chief Information Officer	
Date Approved:	November 2, 2017	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Information Officer	
Contact Name:	Kathy Lyons-Burke	

EXECUTIVE SUMMARY

Management Directive (MD) 12.5, "NRC Cybersecurity Program," is revised to incorporate Controlled Unclassified Information (CUI), reflect current Federal laws and direction, align cybersecurity roles with National Institute of Standards and Technology guidance, and reflect recent NRC organizational changes.

- Clarified the roles and responsibilities for the Insider Threat Program, foreign assignees, and secure video conferencing.
- Replaced policy and guidance regarding the handling of Safeguards information (SGI), or sensitive unclassified non-Safeguards information (SUNSI), with CUI, as appropriate.
- Removed the role of the Designated Approving Authority from the MD to reflect transfer of these roles and responsibilities to the Authorizing Official.
- Exhibit 1 was eliminated.

MD 12.5 is issued in accordance with Commission direction to ensure NRC information is appropriately protected.

TABLE OF CONTENTS

I. POLICY

A. It is the policy of the U.S. Nuclear Regulatory Commission to implement and maintain an agencywide Cybersecurity Program to protect information and information technology (IT) systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability as defined in 44 U.S.C. 3542.

B. NRC cybersecurity protections shall be consistent with Federal guidance and commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of classified information and information that qualifies as Controlled Unclassified Information (CUI) as specified in 32 CFR Part 2002 and IT systems that are operated, maintained, or sponsored by the agency.

C. NRC cybersecurity protections encompass computer-based hardware, software, or associated administrative procedures that are used to process, store, or transmit NRC information whether it is uncontrolled unclassified information (UUI), classified information, or CUI.

D. The Cybersecurity Program shall directly support and enhance the mission and business objectives of the agency, including the capability for NRC to perform its mission in all threat environments. The program shall include policies, planning, budgeting, management, implementation, and oversight.

II. OBJECTIVES

- Implement cybersecurity measures to protect and ensure reliable access to NRC information and IT systems for authorized individuals. Cybersecurity measures include any computer-based hardware, software, or associated administrative and operational procedures that are used to process, store, or transmit NRC information, whether it is UUI, classified information, or CUI.
- Ensure users receive cybersecurity awareness and training.
- Integrate cybersecurity management processes with agency strategic and operational planning processes.
- Ensure office directors and regional administrators provide cybersecurity controls for the IT systems and assets under their control.
- Ensure the secure interoperability and integration of NRC IT systems by ensuring cybersecurity requirements are fully integrated into the NRC Enterprise Architecture (EA).

- Operate and maintain a comprehensive cyber situational awareness capability that includes mitigating actions to prevent cybersecurity incidents.
- Provide adequate cybersecurity for all information created, collected, processed, stored, transmitted, disseminated, or disposed of by or on behalf of the agency, to include Federal information residing in contractor information systems and networks.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Executive Director for Operations (EDO)

The EDO has inherent U.S. Government authority, must be a Government employee, and is responsible for the following as it relates to cybersecurity:

1. Ensures agency compliance with the requirements imposed on the agency by FISMA and related policies, procedures, standards, and guidelines.
2. Ensures that all offices have the necessary resources to comply with the requirements specified in the agencywide Cybersecurity Program.
3. Appoints the agency Chief Information Officer (CIO) and delegates the authority to ensure compliance with the requirements imposed on the agency by FISMA and related policies, procedures, and standards.
4. Ensures that the CIO, in coordination with other senior executives, reports annually on the effectiveness of the agencywide Cybersecurity Program, including progress of remedial actions.
5. Appoints the agency's Authorizing Officials (AOs) and identifies each AO's responsibilities by memorandum.
6. Ensures cybersecurity controls protect information stored, processed, or transmitted by NRC IT systems used or operated by, for, or on behalf of the agency commensurate with the risk and magnitude of the harm that could result from unauthorized access, use, modification, disclosure, disruption, or destruction.
7. Ensures that office directors and regional administrators provide risk-based cybersecurity protections for the information and IT systems that support the operations and assets under their control.
8. Ensures that cybersecurity management processes are integrated with agency strategic and operational planning processes.
9. Ensures that the agency has trained personnel sufficient to assist the agency in complying with FISMA and related policies, procedures, standards, and guidelines.

10. Identifies NRC business lines and the business line leads responsible for those business lines.
11. Enforces the agency implementation of the Cybersecurity Program at the operational level.
12. In conjunction with the CIO and the OMB Administrator of the Office of Electronic Government, conducts an annual review of the agency IT portfolio.

B. Chief Financial Officer (CFO)

Ensures, in partnership with the EDO, that funds are available for essential IT resources, including staffing, so that all offices can comply with the NRC Cybersecurity Program requirements.

C. Inspector General (IG)

1. Investigates, audits, and takes other action in accordance with the Inspector General Act of 1978 (5 U.S.C. App. 3) to prevent and detect misconduct or wrongdoing in connection with the NRC Cybersecurity Program.
2. Conducts an annual independent evaluation of the effectiveness of NRC's information security program and practices.
3. Oversees, evaluates, and supports resolution of compliance issues pertinent to the organization.
4. Inspects and tests IT systems to ensure compliance with cybersecurity policy, procedures, and regulations.
5. Coordinates cybersecurity related investigative matters with other law enforcement organizations.

D. Office of the General Counsel (OGC)

Provides legal advice for cybersecurity matters.

E. Chief Information Officer (CIO)

The CIO has overall responsibility for IT services and implementations used by the agency, including policy, procedures, and control techniques. The CIO has inherent U.S. Government authority, must be a Government employee, and consistent with the EDO appointment, is responsible for the following as it relates to cybersecurity:

1. Ensures the integrity, availability, and confidentiality of NRC's IT systems.
2. Serves a significant role in planning, programming, and budgeting, has input to reporting requirements, management, governance, and oversight processes related to IT.

3. Approves the IT budget request for the agency and certifies that IT investments implement incremental development, as defined in capital planning guidance issued by OMB.
4. Enforces enterprise risk management and provides assurance on internal control effectiveness. Coordinates the implementation of both information security and privacy controls.
5. Monitors the performance of agency IT programs.
   (a) Evaluates the performance of those programs on the basis of the applicable performance measurements.
   (b) Advises the EDO regarding whether to continue, modify, or terminate a program or project.
   (c) Uses agency plans of action and milestones and makes them available or provides access to them to OMB, DHS, inspectors general, and the U.S. Government Accountability Office, upon request, to record and manage the mitigation and remediation of identified weaknesses and deficiencies, not associated with accepted risks, in agency information systems.
6. Approves all contracts or other agreements for IT or IT services.
7. Approves all reprogramming of any funds made available for IT programs.
8. In consultation with other appropriate agency officials, categorizes each IT investment according to risk, in accordance with guidance issued by the EDO.
9. For each high risk IT investment, in consultation with the Administrator of the OMB Office of Electronic Government, reviews the investment to identify the root causes of the high level of risk of the investment; the extent to which these causes can be addressed; and the probability of future success.
10. In conjunction with the EDO and the OMB Administrator of the Office of Electronic Government, conducts an annual review of the agency IT portfolio.
11. Advises and assists office directors and regional administrators on IT acquisition and management.
12. Ensures the implementation and maintenance of a sound, cost-effective, and integrated EA that supports the NRC's mission.
13. Ensures that NRC's IT systems, including Web sites, protect the privacy of the public, businesses, employees, and contractors.
14. Ensures that NRC maintains a workforce of well-qualified cybersecurity professionals.

15. Jointly with the Chief Human Capital Officer (CHCO), identifies all positions within the agency that require the performance of cybersecurity or other cyber-related functions and ensures the correct corresponding employment code is assigned.
16. Establishes, implements, and enforces an agencywide framework to facilitate an incident response program, ensuring proper and timely reporting to the United States Computer Emergency Readiness Team (US-CERT).
17. Appoints the agency Chief Information Security Officer (CISO) and delegates the authority to develop and maintain the agencywide Cybersecurity Program.
18. Approves all connections and agreements (e.g., IT-related interagency agreements) related to connections between an NRC system and another Federal agency system or a system owned by another party.
19. Manages non-IT information security policies for marking, handling, and protecting non-electronic UUI and CUI except CUI Specified-SGI (CUI/SP-SGI).
20. Ensures cybersecurity requirements are properly incorporated into the agency's IT operations and System Development Life Cycle (SDLC) methodology, and system security engineering principles, concepts, and techniques are employed during the SDLC to facilitate the development, deployment, operation, and sustainment of trustworthy and adequately secured systems.
21. Jointly with the Chief Human Capital Officer (CHCO), develops a set of competency requirements for IT staff, including IT leadership positions, and develops and maintains a current workforce planning process to ensure the NRC can (a) anticipate and respond to changing mission requirements, (b) maintain workforce skills in a rapidly developing IT environment, and (c) recruit and retain the IT talent needed to accomplish the mission.
22. Ensures development and maintenance of an agencywide continuous monitoring strategy and ensures continuous monitoring of the cybersecurity state of NRC's IT systems is performed consistently with that strategy.
23. As the Senior Agency Official responsible for CUI, manages and implements the CUI program in accordance with 32 CFR Part 2002, "Controlled Unclassified Information," and manages the NRC's implementation of the CUI program, including the NRC's transition to that program. In this role, the CIO performs the following:

    (a) Ensures that electronic documents not covered by a waiver from the CUI executive agent containing CUI include markings such that when the document is printed or viewed, the markings are evident in accordance with CUI marking requirements.

(b) Ensures that electronic CUI is protected in accordance with CUI requirements.

(c) Ensures electronic CUI is encrypted or rendered indecipherable to unauthorized users while in transit and while stored.

24. Ensures that each NRC public Web site that requires user authentication employs a single sign-on trusted identity platform for individuals accessing the Web site.

25. Ensures multi-factor authentication is employed for all remote access to IT systems and for privileged accounts.

26. Ensures use of federally provided improved intrusion detection and prevention capabilities.

27. Coordinates, reviews, and approves, in conjunction with the Director, Division of Facilities and Security (DFS), Office of Administration (ADM), physical security proposals and plans for buildings and rooms that will be used for processing NRC electronic information.

F. Authorizing Official (AO)

The AO is an individual or committee consisting of senior executives with designated authority to assume formal responsibility for operating an IT system at an acceptable level of risk based on an agreed-upon set of implemented security controls. The AO consists of one or more senior executives with a level of authority commensurate with understanding and accepting these IT system-related security risks. The AO has inherent U.S. Government authority and comprises officials who must be Government employees. The AO performs the following:

1. Assumes responsibility and is accountable through the system security authorization process for the security risks associated with an IT system.

2. Approves or disapproves security plans, memoranda of agreement or understanding, and plans of action and milestones.

3. Authorizes and de-authorizes IT system operations.

4. Halts operations of any IT system when it determines that an unacceptable level of risk exists.

5. Coordinates authorization activities with the CIO, CISO, common control providers, information owners, system owners, security control assessors, and other interested parties during the security authorization process.

6. Delegating authorizing official activities and functions to Authorizing Official Designated Representatives (AODRs).

7. Ensures that all activities and functions delegated to any AODRs are accomplished.
8. Determines the actions necessary to mitigate risks discovered during continuous monitoring, annual assessments, and penetration testing.
9. Authorizes significant system changes and determines if reauthorization is required.
10. Approves deviations from defined security requirements.

G. Chief Information Security Officer (CISO)

The CISO has overall responsibility for the agency's Cybersecurity Program, including policy, procedures, and control techniques. The CISO has inherent U.S. Government authority, must be a Government employee, and is responsible for the following as it relates to cybersecurity:

1. Plans, directs, and oversees the implementation of the agencywide Cybersecurity Program.
2. Provides cybersecurity requirements for electronic information processing, storage, and transmission.
3. Oversees IT contingency planning for the agency.
4. Ensures the agencywide Cybersecurity Program adheres to federally mandated and NRC-defined security requirements.
5. Enforces compliance with the agencywide Cybersecurity Program at the operational level.
6. Ensures that cybersecurity policies, procedures, and control techniques are properly balanced against business objectives, costs, and the need to ensure that cybersecurity is addressed throughout the life cycle of each NRC IT system.
7. Functions as the NRC IT risk executive, ensuring that risk acceptance decisions are consistent across the agency. This includes identifying organizational risk posture based on aggregating risk from individual IT systems and ensuring that cybersecurity is integrated into segmented EAs.
8. Ensures that employees receive periodic cybersecurity refresher training, including awareness, basics, and literacy instruction.
9. Proposes and advocates appropriate agency cybersecurity standards and guidelines.
10. Guides security process maturity within the NRC and advocates these concepts to NRC organizations.

11. Identifies the list of common controls for the agencywide Cybersecurity Program.
12. Serves as the agency's liaison with external entities on mutual cybersecurity interests.
13. Ensures cybersecurity incidents are reported to the Office of the Inspector General (OIG) to determine if criminal investigation is warranted.
14. Approves cybersecurity plans for foreign assignee electronic processing of NRC information. The definition of foreign assignee is provided in MD 12.1, "NRC Facility Security Program."

H. Director, Office of Nuclear Security and Incident Response (NSIR)

1. Manages NRC non-IT information security programs that specifically deal with the classification, declassification, and handling of classified information and safeguards information (CUI/SP-SGI).
2. Ensures security, operation, and maintenance of NRC's classified computing capability, and acts as owner of all classified information systems at the NRC.
3. Ensures secure operation of the classified communications center for organizational messaging and other classified transmissions
4. Ensures the acquisition, distribution, and maintenance of classified phones, faxes, secure video teleconferencing, and other secure equipment and cryptographic keying devices.

I. Office Directors and Regional Administrators

1. Ensure that all employees and contractors with assigned security and privacy roles and responsibilities complete cybersecurity training in accordance with their role before assuming the role and at required intervals.
2. Ensure that all users complete required cybersecurity awareness courses and acknowledge the rules of behavior.
3. Ensure that NRC IT-related interagency agreements, with the required Interconnection Security Agreement, are submitted to the CIO for approval.
4. Ensure that IT investments are approved by the CIO prior to acquisition.
5. Ensure that implementation of IT (e.g., hardware, software, and firmware) be authorized by the NRC AO before it is used for NRC purposes or connected to NRC resources.

J. Chief Human Capital Officer (CHCO)

1. Jointly with the CIO, develops a set of competency requirements for IT staff, including IT leadership positions, and develop and maintain a current workforce planning process to ensure the department/agency can accomplish the following:

   (a) Anticipate and respond to changing mission requirements,

   (b) Maintain workforce skills in a rapidly developing IT environment, and

   (c) Recruit and retain the IT talent needed to accomplish the mission.

2. Jointly with the CIO, identifies all positions within the agency that require the performance of cybersecurity or other cyber-related functions and ensures the correct corresponding employment code is assigned.

3. Provides assistance in the development and delivery of the cybersecurity awareness and role-based training program for NRC IT users. Provides other cybersecurity-related training as requested.

4. Maintains cybersecurity-related training records for NRC IT users.

5. Maintains role-based training records for NRC personnel (for example: general users, system administrators, Information System Security Officers (ISSO), and users with significant IT responsibilities).

6. Ensures that a cybersecurity briefing is included in the initial orientation for new employees.

7. Notifies the CIO of NRC staff terminations and transfers.

K. Director, Office of Administration

1. Serves as the Senior Agency Official for the Insider Threat Program.

2. Approves banner language for all electronic devices and computer networks to ensure compliance with Executive Order 13587 and the Insider Threat Program.

L. Director, Division of Facilities and Security (DFS), Office of Administration (ADM)

1. Ensures that appropriate buildings and rooms are provided for NRC IT systems, and participates in planning, installation, and operations and maintenance of those buildings and rooms.

2. Coordinates, reviews, and approves, in conjunction with OCIO, physical security proposals and plans for buildings and rooms that will be used for processing NRC electronic information.

3. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC personnel security program, including clearing personnel so that system owners can authorize their access to NRC IT systems.
4. Administers the NRC's Insider Threat Program in coordination with other designated NRC offices.
5. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC Facility Security Program including the review, survey and approval of facilities and spaces for handling, receiving, storage, transmitting, processing, and protecting of classified, UUI, CUI Basic, and CUI Specified data and information.
6. Administers and issues Personnel Identification Verification (PIV) cards to comply with Homeland Security Presidential Directive 12.
7. Conducts surveys and approves spaces that receive, process, transmit, or protect classified data or information including non-NRC facilities that handle UUI, CUI, and classified information.
8. Destroys sensitive IT equipment.
9. Reviews and approves all security plans for Foreign Assignees in accordance with MD 12.1.

M. Director, Acquisition Management Division (AMD), Office of Administration (ADM)

Ensures that Federal and NRC requirements for information protection, system availability, and continuity of operations, as documented in Volume 12 of the NRC MD catalog, are included in solicitations and contracts for the design, development, acquisition, or operation and maintenance of IT systems.

IV. APPLICABILITY

The policy and guidance in this directive and handbook apply to all NRC employees, support contractors, and other users that authenticate to NRC systems and who process, store, or produce UUI, classified information, or CUI using IT systems or IT facilities that are under the security jurisdiction of the NRC.

V. DIRECTIVE HANDBOOK

Handbook 12.5 facilitates implementation of the NRC Cybersecurity Program. The handbook includes guidance regarding administrative, technical, management, operational, and physical security measures appropriate for the protection of NRC IT facilities and systems, and classified national security information, UUI, and CUI processed, stored, or transmitted using an NRC IT system.

VI. GUIDANCE DOCUMENTS

A. Safeguarding of Non-electronic Classified Information

MD 12.2, “NRC Classified Information Security Program,” pertains to the classification of classified information, requirements for obtaining access to classified information, and safeguarding of non-electronic classified information.

B. Safeguarding of Non-Electronic Safeguards Information (CUI/SP-SGI)

MD 12.7, “NRC Safeguards Information Security Program,” pertains to the designation of CUI/SP-SGI, requirements for obtaining access to CUI/SP-SGI, and the safekeeping and storage requirements for non-electronic CUI/SP-SGI.

C. Safeguarding of Non-Electronic Controlled Unclassified Information (CUI)

As the Federal Government's Executive Agent for CUI, the National Archives and Records Administration (NARA), through its Information Security Oversight Office (ISOO), oversees the Federal Government-wide CUI Program. As part of that responsibility, ISOO has issued rule 32 CFR Part 2002, “Controlled Unclassified Information,” to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program. The rule and marking guidance can be viewed on the CUI Web site (also called the CUI Registry) at https://www.archives.gov/cui.

D. Glossary

MD 12, “Glossary of Security Terms,” is a listing of defined security terms used in the MD Volume 12, “Security,” series.

VII. FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) AND OTHER FEDERAL GUIDANCE

FISMA directs the Department of Commerce, NIST, to prescribe standards and guidelines pertaining to cybersecurity. These standards and guidelines are required at NRC for unclassified systems. The NRC shall follow NIST guidance to the maximum extent practicable, ensuring that such standards and guidelines provide for sufficient flexibility to permit alternative solutions that provide equivalent levels of protection for identified cybersecurity risks. Compliance with NIST standards and guidelines includes information pertaining to the preparation of documentation (including system security plans, IT risk assessments, and IT contingency plans) and other applicable NIST guidance for cybersecurity processes, procedures, and testing. FISMA also directs agencies to implement information security policies and practices as required by standards and

guidelines for national security systems issued in accordance with law and as directed by the President. Currently, the guidelines and standards for national security systems are issued by the CNSS, Director of National Intelligence (DNI), and system owners. The NRC shall comply with the CNSS and DNI policy and guidance to include guidance related to the preparation of cybersecurity documentation and other applicable CNSS guidance for cybersecurity processes, procedures, and testing.

VIII. INFORMATION TECHNOLOGY ROLES AND RESPONSIBILITIES

A. System Owner

A system owner is an office director, regional administrator, or OCIO division director that has overall responsibility for the security of NRC systems owned by his or her organization or operated on behalf of his or her organization by another agency or by a contractor. The system owner is a government employee who has inherent U.S. Government authority.

B. Common Control Provider

A common control is a security control that is inherited by one or more IT systems. A common control provider is an office director, regional administrator, or OCIO division director with overall responsibility for the development, implementation, assessment, and monitoring of a set of common controls. Common control providers, as the system owners for these systems, are accountable for the security risk associated with operating his/her system/common controls. The common control provider is a government employee who has inherent U.S. Government authority.

C. Information Owner

An information owner has authority for specific information and responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. The owner/steward provides rules for appropriate use and protections of the subject information and provides input to system owners regarding the system requirements and security controls where the information is processed, stored, or transmitted. The information owner is a Government employee who has inherent U.S. Government authority.

IX. EXCEPTIONS

Exceptions to or deviations from this directive and handbook may be granted by the AO, except for those areas in which the responsibility or authority is vested solely with the EDO or ADM and cannot be delegated, or for matters specifically required by law, Executive Order, or directive to be referred to other management officials. For national security systems, nothing in this directive and handbook shall supersede any authority of the DNI, NSA, Secretary of

Defense, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems. Nothing in this directive or handbook shall supersede any requirement made by or under the Atomic Energy Act of 1954. Restricted data or formerly restricted data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954.

X. REFERENCES

Code of Federal Regulations

10 CFR Part 73, "Physical Protection of Plants and Materials."

32 CFR Part 2001, "Classified National Security Information."

32 CFR Part 2002, "Controlled Unclassified Information."

Committee on National Security Systems

CNSS Policies Web Site:
https://www.cnss.gov/CNSS/issuances/Policies.cfm.

CNSS Directives Web Site:
https://www.cnss.gov/CNSS/issuances/Directives.cfm.

CNSS Instructions Web Site:
https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

CNSS Web Site:
http://www.cnss.gov.

CNSS Instruction (CNSSI) 1253, "Security Categorization and Control Selection for National Security Systems."

Executive Order (EO)

EO 13526, "Classified National Security Information," December 29, 2009.

EO 13556, "Controlled Unclassified Information," November 4, 2010.

EO 13681, "Improving the Security of Consumer Financial Transactions," October 17, 2014.

EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.

Government Accountability Office (GAO)

GAO-15-593SP, "A Framework for Managing Fraud Risks in Federal Programs," July 2015.

GAO-14-704G, "Standards for Internal Control in Federal Government (GREEN BOOK 2014)," September 2014.

Homeland Security Presidential Directive (HSPD)

Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.

International Standards

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Standard 27002:2005(E), "Code of Practice for Information Security Management," June 15, 2005.

United States Computer Security Readiness Team (US-CERT) Federal Incident Reporting Guidelines, available at http://www.us-cert.gov/.

National Archives

National Archives Controlled Unclassified Information Web Site (also the CUI Registry):
https://www.archives.gov/cui.

National Institutes of Standards and Technology

NIST Computer Security Division, Computer Security Resource Center:
http://csrc.nist.gov.

NIST Federal Information Processing Standards (FIPS) Publications:
http://csrc.nist.gov/publications/PubsFIPS.html.

NIST Publications:
http://csrc.nist.gov/publications/.

FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems."

FIPS PUB 140-2, "Security Requirements for Cryptographic Module."

NIST Special Publications (SP):
http://csrc.nist.gov/publications/PubsSPs.html.

NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach."

NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."

NIST SP 800-59, “Guideline for Identifying an Information System as a National Security System.”

NIST SP 800-61, “Computer Security Incident Handling Guide.”

NIST SP 800-64, “Security Considerations in the System Development Life Cycle.”

NIST SP 800-88, “Guidelines for Media Sanitization.”

NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems.”

NIST SP 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations.”

NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.”

Nuclear Regulatory Commission Documents

“Agencywide Rules of Behavior for Authorized Computer Use,” available at http://www.internal.nrc.gov/CSO/documents/ROB.pdf.

Management Directives (MD)

MD 2.7, “Personal Use of Information Technology.”

MD 2.8, “Integrated Information Technology/Information Management (IT/IM) Governance Framework.”

MD Vol. 3, “Information Management,” Part 2, “Records Management.”

MD 3.51, “Library Services.”

MD 3.52, “Availability and Retention of Codes and Standards.”

MD 3.53, “NRC Records and Document Management Program.”

MD 3.54, “NRC Information Collections Program.”

MD 3.55, “Forms Management Program.”

MD 3.57, “Correspondence Management.”

MD 7.4, “Reporting Suspected Wrongdoing and Processing OIG Referrals.”

MD 10.166, “Telework.”

MD 12, “Glossary of Security Terms.”

MD 12.1, “NRC Facility Security Program.”

MD 12.2, “NRC Classified Information Security Program.”

MD 12.3, “NRC Personnel Security Program.”

MD 12.4, “NRC Communications Security (COMSEC) Program.”

MD 12.7, “NRC Safeguards Information Security Program.”

MD 13.1, “Property Management.”

NRC Cybersecurity Documents

OCIO Cybersecurity Web Site:
http://www.internal.nrc.gov/CSO/.

Checklists:
http://www.internal.nrc.gov/CSO/checklists.html.

Cybersecurity Guidance:
http://www.internal.nrc.gov/CSO/guidance.html.

Cybersecurity Incident Response:
http://www.internal.nrc.gov/CSO/incident-resp.html.

Cybersecurity Policies:
http://www.internal.nrc.gov/CSO/policies.html.

Cybersecurity Procedures:
http://www.internal.nrc.gov/CSO/procedures.html.

Cybersecurity Processes:
http://www.internal.nrc.gov/CSO/processes.html.

Cybersecurity Standards:
http://www.internal.nrc.gov/CSO/standards.html.

Cybersecurity Templates:
http://www.internal.nrc.gov/CSO/security_templates.html.

NRC General User Remote Access Cybersecurity Checklist:
http://www.internal.nrc.gov/CSO/checklists.html.

NRC/National Treasury Employees Union (NTEU)
Collective Bargaining Agreement:
http://www.internal.nrc.gov/HR/.

NRC Personally Identifiable Information (PII) Guidance:
http://www.internal.nrc.gov/CSO/divisions/irsd/privacy/index.html.

NRC Telework Information:
http://www.internal.nrc.gov/HR/telework.html.

Office of Management and Budget Documents (OMB)

OMB Circular A-11, "Preparation, Submission and Execution of the Budget," July 1, 2016.

OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016.

OMB Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016.

OMB Memoranda (M), available at https://www.whitehouse.gov/omb/memoranda/.

OMB M-16-24, "Role and Designation of Senior Agency Officials for Privacy," September 15, 2016.

OMB M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 19, 2017.

United States Code

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

Cybersecurity Enhancement Act of 2014, Pub. L. 113–4 274 (15 U.S.C. 7464).

Cybersecurity Act of 2015, Pub. Law 114-113, div. N, Dec. 18, 2015.

Gathering, Transmitting or Losing Defense Information (18 U.S.C. 793).

Federal Information Security Modernization Act (FISMA) of 2014
(44 U.S.C. 3541 et seq.).

Federal Information Technology Acquisition Reform Act (FITARA), Pub. L. 113-291.

Inspector General Act (5 U.S.C. App. 3).

Federal Managers Financial Integrity Act (FMFIA) of 1982, Pub. L. 97-255, H.R. 1526.

DH 12.5	NRC CYBERSECURITY PROGRAM	DT-17-16
Volume 12:	Security	
Approved by:	David J. Nelson Chief Information Officer	
Date Approved:	November 2, 2017	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Information Officer	
Contact Name:	Kathy Lyons-Burke	

EXECUTIVE SUMMARY

Management Directive (MD) 12.5, "NRC Cybersecurity Program," is revised to incorporate Controlled Unclassified Information (CUI), reflect current Federal laws and direction, align cybersecurity roles with National Institute of Standards and Technology guidance, and reflect recent NRC organizational changes.

- Clarified the roles and responsibilities for the Insider Threat Program, foreign assignees, and secure video conferencing.
- Replaced policy and guidance regarding the handling of Safeguards information (SGI), or sensitive unclassified non-Safeguards information (SUNSI), with CUI, as appropriate.
- Removed the role of the Designated Approving Authority from the MD to reflect transfer of these roles and responsibilities to the Authorizing Official.
- Exhibit 1 was eliminated.

MD 12.5 is issued in accordance with Commission direction to ensure NRC information is appropriately protected.

TABLE OF CONTENTS

EXHIBIT

I. NRC CYBERSECURITY PROGRAM

A. Introduction

The U.S. Nuclear Regulatory Commission Cybersecurity Program protects NRC information and information technology (IT) systems from unauthorized access, use, disclosure, disruption, modification, and destruction. The Cybersecurity Program determines the threats to NRC's IT resources, defines the vulnerabilities related to those threats, and then mitigates risks in light of the mission needs. All electronic information processing, storage, and transmission must comply with MD 12.5.

1. Definitions

(a) Information security is defined as protection of the confidentiality, integrity, and availability of information from unauthorized access, use, disclosure, disruption, modification, or destruction.

(b) Cybersecurity is the application of information security to IT systems to ensure availability, integrity, authentication, confidentiality and non-repudiation. It includes damage prevention and restoration activities.

(c) Controlled Unclassified Information (CUI) is unclassified information that requires protection or dissemination control. Regulations in 32 CFR Part 2002, "Controlled Unclassified Information," mandate that authorized holders protect CUI using CUI Basic or CUI Specified controls. The regulations also require the CUI Executive Agent (EA) to establish and maintain a Federal Governmentwide CUI registry to provide authorized categories, subcategories, associated markings, as well as applicable safeguarding, dissemination, and decontrol procedures for CUI. Dissemination controls,

CUI marking handbook, and additional tools are available at the CUI Web site (also called the CUI Registry) at https://www.archives.gov/cui.

(i) CUI Basic is the subset of CUI for which the authorizing law, regulation, or Governmentwide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic per the uniform set of controls in the 32 CFR Part 2002 and the CUI Registry. All CUI Basic categories are controlled at the "moderate" confidentiality level at a minimum.

(ii) CUI Specified (CUI/SP) is the subset of CUI for which the authorizing law, regulation, or Governmentwide policy contains specific handling controls that it requires or permits agencies to use that are in addition to those for CUI Basic. The CUI Registry indicates which laws, regulations, and Governmentwide policies include such specific requirements. CUI Specified information may be handled at higher confidentiality levels if the authorities establishing and governing the CUI Specified allow or require more specific or stringent controls. Safeguards Information (SGI) is considered to be CUI/SP-SGI and requires more stringent controls than CUI Basic.

(iii) Uncontrolled Unclassified Information (UUI) is information that is neither CUI nor classified information. UUI must be handled in accordance with Federal Information Security Modernization Act (FISMA) requirements in accordance with 32 CFR Part 2002.

2. Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. 3541 et seq.)

   FISMA directs agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of (1) information collected or maintained by or on behalf of an agency, or (2) IT systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

3. Components of the NRC Cybersecurity Program

   (a) Policies and procedures that are based on formal assessments of risk;

   (b) Subordinate plans for providing adequate cybersecurity for networks, facilities, IT systems, and groups of IT systems;

   (c) Periodic assessments of risk;

   (d) A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in NRC cybersecurity policies, procedures, and practices;

   (e) Plans and procedures to ensure continuity of operations for IT systems that support NRC operations and assets;

(f) Periodic testing and evaluation of the effectiveness of cybersecurity policies, procedures, practices, and security controls;

(g) Security awareness and training to inform personnel of the cybersecurity risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks; and

(h) Procedures for detecting, reporting, and responding to cybersecurity incidents.

4. The Office of Management and Budget (OMB) principles that guide the efforts to incorporate security and privacy into NRC IT systems are as follows:

(a) Effective security for protecting information is an essential element of all NRC IT systems, regardless of the classification or sensitivity of the information being processed.

(b) Effective privacy protections are essential to all NRC IT systems, especially those that contain substantial amounts of personally identifiable information (PII). The use of new information technologies should sustain, and not erode, the privacy protections provided in all statutes and policies relating to the collection, use, and disclosure of personal information. NRC shall require, as appropriate, other agencies and entities with which it shares PII to maintain the PII in an information system with an appropriate confidentiality impact level.

(c) The increase in efficiency and effectiveness that flows from the use of interconnected computers and networks has been accompanied by increased risks. The protection of NRC IT systems resources must be commensurate with the risk of harm resulting from any misuse or unauthorized access to these systems and the information stored, processed, or transmitted on them.

(d) Security risks and incidents must be managed in a way that complements and does not unnecessarily impede agency business operations. By understanding risks and implementing an appropriate level of controls, NRC can significantly reduce risk and potential loss.

(e) A strategy to manage security is essential. This strategy should be based on an ongoing cycle of risk management and shall be described in system security plans. The strategy should identify significant risks, clearly establish responsibility for reducing them, and ensure that risk management remains effective over time.

(f) NRC must understand the risk to systems under NRC control and determine the acceptable level of risk, ensure that adequate security is maintained to support and assist the programs under NRC control, and ensure that security controls support program needs and appropriately accommodate operational necessities. In addition, security measures shall support the agency enterprise and security architectures.

B. Structure of the Handbook

This handbook follows the internationally accepted information security policy framework identified in International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 27002:2005, "Code of Practice for Information Security Management." This handbook consists of the following 11 sections:

1. Section I: NRC Cybersecurity Program – Identifies the NRC Cybersecurity Program requirements.
2. Section II: Organization of Cybersecurity – Defines the framework that controls the implementation of cybersecurity within NRC.
3. Section III: Information Technology Asset Management – Identifies requirements for NRC IT asset management.
4. Section IV: Personnel – Identifies personnel security requirements related to cybersecurity.
5. Section V: Physical and Environmental Security – Identifies physical security and environmental security requirements related to cybersecurity.
6. Section VI: Communications and Operations Management – Identifies requirements for the correct and secure operation of IT facilities.
7. Section VII: Access Control – Identifies requirements to control access to information and IT systems.
8. Section VIII: IT Systems Acquisition, Development, and Maintenance – Identifies requirements for security to be an integral part of IT systems.
9. Section IX: Cybersecurity Incident Management – Identifies requirements for reporting and mitigating security events and weaknesses associated with IT systems.
10. Section X: Business Continuity Management – Identifies requirements to counteract interruptions to business activities and protect business processes from major failures and disasters.
11. Section XI: Compliance – Identifies requirements to avoid breaches of legal, statutory, regulatory, or contractual obligations and of any security requirements.

C. Authorities and Other Guidance

1. The references provided in Section X of this MD provide additional authority for the NRC Cybersecurity Program. FISMA also directs the Department of Commerce, NIST, to prescribe standards and guidelines pertaining to IT systems that do not process classified information. These NIST standards are mandatory within the agency. NIST cybersecurity information is available at http://csrc.nist.gov and also can be obtained by contacting the Office of the Chief Information Officer (OCIO)/Information Security Planning and Oversight (ISPO) staff. NIST issues this information in the form of Federal Information Processing Standards (FIPS) and Special Publications (SP), which were considered in the preparation of this handbook.

2. Systems compliance is described as follows:

   (a) Systems that process UUI or CUI must comply with 32 CFR Part 2002, "Controlled Unclassified Information."

   (b) Systems that process classified information must comply with Committee on National Security Systems (CNSS) direction. The CNSS Web site is located at http://www.cnss.gov.

   (c) Systems that process Sensitive Compartmented Information (SCI) must adhere to Director of National Intelligence (DNI) policy, standards, and guidance. The DNI Web site is located at http://www.dni.gov/.

3. System owners should consult with the CIO for information related to SCI electronic processing.

4. The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is a Governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP solutions are authorized by the Joint Authorization Board (JAB). Additional information is available on the FedRAMP Web site at https://www.fedramp.gov/. FedRAMP authorizations can be used by NRC in accordance with Section I.E, "Authorization to Use Process."

5. OCIO provides additional direction for cybersecurity in the form of standards, processes, procedures, and guidelines. OCIO cybersecurity direction can be found on the OCIO cybersecurity Web site at http://www.internal.nrc.gov/CSO/.

6. Some OCIO cybersecurity issuances are mandatory and some are advisory; each type goes through its own approval process. These differences are detailed as follows:

   (a) NRC cybersecurity standards are mandatory and are developed and approved by the AO. Standards generally define items like mandatory agencywide software configurations and technology specifications.

   (b) NRC cybersecurity procedures are mandatory and are developed and approved by the OCIO/ISPO in coordination with appropriate office directors through the Information System Security Officer (ISSO) Forum. Procedures are based on this policy and generally define business processes that have agencywide security implications.

   (c) NRC cybersecurity guidelines are not mandatory, are developed by the OCIO/ISPO in coordination with and approved by the Chief Information Security Officer (CISO), and generally provide agencywide guidance for the implementation of security best practices within the NRC.

7. OCIO/ISPO standards, processes, procedures, and guidelines may address infrastructure that supports all of the NRC or address specific items that may or may not be applicable to the entire agency. Therefore, in addition to this handbook, users

must be aware of other guidance that may affect the use of IT systems within the NRC. All cybersecurity guidance is available on the OCIO cybersecurity Web site at http://www.internal.nrc.gov/CSO/.

8. Some cybersecurity guidance documents are specific to a particular system. Various offices and system owners within NRC develop this type of guidance as they develop operational and business processes that include security. For example, system-specific procedures are the responsibility of system owners. Those system owners also are responsible for ensuring that system-specific procedures are available to users and for ensuring all developed procedures are compliant with MD 12.5.

D. Authorization to Operate Process

1. An IT system is authorized for operation at a specific point in time based on the risk associated with the current security state of the system. NIST, the U.S. Department of Defense (DOD), and the intelligence community have collaborated in the development of a Governmentwide system authorization process. This process is an integral part of the system development life cycle (SDLC) and the Risk Management Framework (RMF). The authorization process provides a well-defined and comprehensive process to ensure that responsibility and accountability for managing IT system-related security risks are determined and assigned appropriately. More information can be found on the NIST FISMA Implementation Web site at http://csrc.nist.gov/groups/SMA/fisma/.

2. The Office of Administration (ADM), Division of Facilities and Security (DFS also ADM/DFS), also must survey any system that receives, processes, transmits, or protects classified data or information in accordance with the requirements and procedures of MD 12.1, "NRC Facility Security Program." The Director of ADM, DFS, must furnish a statement of any proposed corrective actions resulting from the survey results to the responsible headquarters office, division, regional office, or contractor.

3. The IT risk executive function is assigned to the CISO. This function integrates with security authorization to accomplish the following:

   (a) Provide consistency across the agency,

   (b) Reflect the agency's risk tolerance, and

   (c) Perform as part of an agencywide process that considers other agency risks affecting mission or business success.

4. In order to be most effective, IT system monitoring activities are integrated into all life cycle management processes carried out by the organization and not executed as standalone, security-centric activities.

5. The SDLC process, including obtaining an Authorization to Operate (ATO), is described in Section VIII.D, "Security in the System Development Life Cycle (SDLC): Risk Management Framework (RMF)," of this handbook.

6. An ATO can be obtained through the Authorization to Use process for systems authorized by another Federal entity.

E. Authorization to Use Process

1. The Authorization to Use (ATU) process is used when another Federal entity has authorized a system or service or application (e.g., FedRAMP authorization).
2. When a system owner wants to use a system authorized by another Federal entity, the system owner ensures the following steps are performed:
   (a) The NRC information types that will be used with the system are identified.
   (b) A security categorization is performed for the NRC information types, and the security categorization is compared to the authorized system's security categorization.
   (c) The authorized capabilities are compared with the capabilities NRC needs.
   (d) The additional cybersecurity controls required to meet NRC requirements and needs, if any, are implemented and independently assessed.
   (e) An authorization package with this information is provided to the AO.
   (f) The AO either accepts or rejects the risk associated with using the system for NRC purposes.

F. Personal Use Systems

NRC authorizations are required only for systems that support the NRC mission. Some Governmentwide services need not undergo an NRC authorization; these include services that collect and process information provided by an NRC employee for the exclusive benefit and use of the employees, and do not support NRC lines of business, such as Employee Express. NRC does not use information from these systems as the basis for any official decision or mission support, and no NRC staff have access to the information for NRC purposes.

G. Managing Risk

1. The foundation of the NRC Cybersecurity Program rests on the identification and management of risk. The program provides the following:
   (a) Determines threats to the NRC's IT resources,
   (b) Defines the vulnerabilities related to those threats, and
   (c) Mitigates risks in light of the mission needs, the business case, good security practices, Government and agency governance, and contractual and legal requirements.
2. FISMA requires the head of each Federal agency to determine "the levels of information security appropriate to protect information and IT systems." To effectively perform this function, NRC considers the following factors:
   (a) The importance of the IT system and the information stored on, processed, or transmitted by that system;

(b) The threats against the IT system;

(c) The likelihood of the threat being applied to the system;

(d) The damage to human life or property, NRC reputation, NRC financial loss, harm to NRC programs, or civil/criminal liabilities that could occur by a compromise of the confidentiality, integrity, or availability of the information stored, processed, or transmitted by the system;

(e) Actions that protect against the threats; and

(f) Costs associated with risk mitigation.

3. Senior executives, known collectively as the AO, decide whether the risks are acceptable.

4. NIST has published guidance, including documents on risk management, to help agencies standardize their approach. These documents are available on the NIST Web site at http://csrc.nist.gov/publications/.

H. Defense-in-Depth

When using this handbook as a guide to establish or administer a security environment for an IT system, defense-in-depth should be the primary approach. Specifically, the system owner should establish multiple layers of security protection to mitigate the impact of an independent security control failure.

I. Waivers and Exceptions

1. When existing policy presents an unacceptable barrier to the accomplishment of business requirements, the system owner may submit a written request to the AO to waive a particular policy requirement. OCIO/ISPO in coordination with the CISO will review these requests and make a written recommendation to the AO regarding the request. The AO makes the final determination regarding a policy waiver and indicates if the waiver is a one-time, single purpose waiver, or if the waiver will become a modification to MD 12.5. OCIO/ISPO tracks waiver decisions and will incorporate them, as appropriate, into future updates of MD 12.5.

2. The system owner may obtain approval to bypass specific cybersecurity requirements from division level management, or above, for a specific instance of emergency or quick turn-around circumstances where meeting the mission in a critical timeframe is essential.

J. Reporting Violations

Anyone who violates or witnesses a violation of NRC cybersecurity policy must report the incident to the CISO by e-mail at CISO@nrc.gov.

K. Electronic Information Requirements

All electronic information processing, storage, transmission, and destruction must comply with MD 12.5.

II. ORGANIZATION OF CYBERSECURITY

A. Internal Organization

MD 12.5 provide the management framework for the NRC Cybersecurity Program.

1. The OCIO is responsible for the following:

   (a) Plans, directs, and oversees the implementation of a comprehensive, coordinated, integrated, and cost-effective NRC Cybersecurity Program, consistent with applicable laws and regulations, and direction, management initiatives, and policies from the Commission, the Executive Director for Operations (EDO), and the Chief Information Officer (CIO).

   (b) Enforces compliance at the operational level.

   (c) Ensures that cybersecurity policies, procedures, and control techniques are balanced against business objectives, costs, and the need to ensure that cybersecurity is addressed throughout the life cycle of each NRC IT system.

2. Management Commitment to Cybersecurity

   NRC management at all levels must ensure the following:

   (a) Cybersecurity requirements are identified for IT systems for which they are responsible and that adequate resources are obligated to meet these requirements.

   (b) All IT systems meet the requirements identified within MD 12.5 and support the agency mission.

   (c) IT processes and procedures reflect cybersecurity requirements identified within MD 12.5.

   (d) The process for authorizing IT systems to operate is an integral part of the SDLC and the RMF.

   (e) An IT risk executive function is incorporated into the security authorization process to ensure that management of IT system-related security risks:

      (i) Is consistent across the NRC,

      (ii) Reflects agencywide risk tolerance, and

      (iii) Is performed as part of an organization-wide process that considers other agency risks affecting mission or business success.

   (f) System authorization is part of a methodical, yet dynamic, risk management process.

3. Cybersecurity Coordination

   The Cybersecurity Program is led by OCIO and coordinated across the agency by personnel assigned to cybersecurity roles. The NRC cybersecurity roles are described in MD 12.5.

4. Delegation of Cybersecurity Responsibilities

   MD 12.5 identifies cybersecurity responsibilities across the NRC. Individuals with assigned security responsibilities may delegate security tasks; however, those individuals retain ultimate responsibility for cybersecurity and must ensure that all delegated tasks are correctly performed. The explicit acceptance of risk is the responsibility of the AO and cannot be delegated to other officials within the organization.

5. Remote Access Computing

   (a) Staff may perform NRC electronic processing from other than NRC facilities with approval from their management in accordance with agency policy, including MD 10.166, "Telework," and the "Collective Bargaining Agreement between U.S. Nuclear Regulatory Commission and National Treasury Employees Union."

   (b) The electronic processing of NRC data from other than NRC facilities is authorized, but is restricted as follows:

      (i) CUI/SP-SGI and classified information must not be processed at facilities that do not have specific authorization for electronic processing of the information. Only facilities specifically approved by ADM/DFS for processing this type of information may be used.

      (ii) Processing of UUI and CUI Basic from other than NRC facilities is permitted when using NRC-approved methods for accessing or processing this type of data. CSO-CKLT-1003, "NRC General User Remote Access Computer Security Checklist," available at http://www.internal.nrc.gov/CSO/checklists.html, provides the required checklist for remote access. Additional information about telework can be found in Section VI.B.3 of this handbook and at http://www.internal.nrc.gov/HR/telework.html.

      (iii) Processing of CUI Specified that is not CUI/SP-SGI from other than NRC facilities is permitted with supervisor approval where authorizing laws, regulations, NRC policies, and Governmentwide policies permit, and when using NRC-approved methods for accessing or processing this type of data. CSO-CKLT-1003, "NRC General User Remote Access Computer Security Checklist," available at http://www.internal.nrc.gov/CSO/checklists.html, provides the required checklist for remote access. Additional information about telework can be found in Section VI.B.3 of this handbook and at http://www.internal.nrc.gov/HR/telework.html.

6. Contact with Authorities

   (a) Cybersecurity Incident Response Team (CSIRT)

   All potential cybersecurity incidents must be reported to the Cybersecurity Incident Response Team (CSIRT) within 1 hour of discovery. The CSIRT is headed by the OCIO/IT Services Development and Operations Division (ITSDOD). The OCIO/ITSDOD Director and CISO will be informed by the CSIRT of the potential cybersecurity incident; the CISO will advise the Inspector General, who will assess whether or not to address the incident. If an investigation is required, the NRC Office of the Inspector General (OIG) will work with other law enforcement agencies as needed to close the incident. Additional information on cybersecurity incident management can be found in Section IX of this handbook. The CSIRT also reports cybersecurity incidents to the United States Computer Emergency Readiness Team (US-CERT) when appropriate. The CISO briefs the CIO on the severity and impact of the incident to the agency.

   (b) CIO and CISO

   Liaison with relevant cybersecurity authorities outside the agency is the responsibility of the CIO and CISO.

   (c) System Owners

   System owners must ensure all federally mandated and NRC-defined cybersecurity requirements have been addressed by their systems. If the boundary of an IT system lies outside of an NRC facility, the system owners must coordinate with the appropriate parties to ensure NRC data and IT resources are properly protected by external parties (e.g., contractors or other Government agencies).

7. Contact with Cybersecurity Special Interest Groups

   The OCIO is the NRC liaison with special interest groups that have an interest in cybersecurity. Other NRC organizations may participate as necessary after coordination with the OCIO. OIG, as part of its statutory law enforcement authority, will interact with other law enforcement agencies and special interest groups and will coordinate information developed with OCIO, as necessary.

B. NRC Roles and Responsibilities for Security Contacts

1. System Owner

   The system owner is responsible for the security of an NRC IT system and is accountable for the security risk associated with operating his or her system. The system owner is responsible for the following:

   (a) Ensuring that each IT system complies with the requirements of MD 12.5.

   (b) Ensuring all new IT procurements include requirements to comply with this policy.

(c) Ensuring that security requirements and planning are included in life cycle budgets for IT systems and in project screening forms and business cases that are completed in accordance with the Capital Planning and Investment Control (CPIC) policy.

(d) Identifying sensitive and mission critical data stored on the system.

(e) Assessing access controls to the data stored on the system, the need for readily accessible storage of the data, and individuals' need to access the data.

(f) Encrypting or otherwise rendering sensitive and mission critical data stored on or transiting the system indecipherable to unauthorized users.

(g) Implementing identity management consistent with Section 504 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–4 274; 15 U.S.C. 7464), including multi-factor authentication, for—

(i) Remote access to the system; and

(ii) Each user account with elevated privileges on the system.

(h) Ensuring at least the minimum control requirements are applied, and additional controls are applied where appropriate.

(i) Ensuring all implementations (e.g., scripts, code, databases) receive an authority to operate from the AO before being put into operation.

(j) Ensuring that all systems and services identified in the Domain Name System (DNS) are protected with Domain Name System Security (DNSSEC) and that all systems are capable of validating DNSSEC protected information.

(k) Appointing an ISSO and alternate ISSO for each system.

(l) Ensuring that required security documentation is prepared and maintained for each system and that each system is deployed and operated in accordance with the agreed-upon security controls.

(m) Providing IT inventory information to OCIO for each IT system that—

(i) Identifies all system hardware, including model identification.

(ii) Identifies all software for each system hardware component, including version identification.

(n) Developing supply chain risk management plans as described in NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," to ensure the integrity, security, resilience, and quality of information systems.

(o) Implementing supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the SDLC.

(p) Identifying each application that is publicly accessible and provides that information to OCIO along with identification of the system and hardware component where the application resides.

(q) Ensuring that access to each publicly accessible application is provided through a secure connection (i.e., hypertext transfer protocol secure (HTTPS)).

(r) Implementing a single sign-on trusted identity platform for individuals accessing each public Web site of the agency that requires user authentication. Ensures that identity proofing, registration, and authentication processes provide assurance of identity consistent with security and privacy requirements, in accordance with Executive Order (EO) 13681, "Improving the Security of Consumer Financial Transactions," OMB policy, and NIST standards and guidelines.

(s) Working in conjunction with the OCIO/ISPO to assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or computer systems under their control and implement policies, procedures, and security controls to cost-effectively reduce risk to an acceptable level.

(t) Performing continuous monitoring of system cybersecurity controls to determine if they are operating as intended and having the desired effect.

(u) Ensuring that, in a timely manner, the NRC CIO and Senior Agency Official for Privacy (SAOP) are made aware of information systems and components that cannot be appropriately protected or secured and that such systems are given a high priority for upgrade, replacement, or retirement.

2. System Owner Designated Representative (SODR)

The system owner designated representative (SODR) is a direct report to the system owner that acts on behalf of the system owner. The system owner must formally appoint the SODR using the CSO-TEMP-0003, "System Owner Designated Representative Appointment Memo," available at http://www.internal.nrc.gov/CSO/security_templates.html. The SODR can perform all activities that a system owner can perform.

3. Common Control Provider

A common control provider is responsible for the security of a specific set of common security controls used to protect multiple IT systems. The common control provider is accountable for the security risk associated with operating his or her common controls. The common control provider is responsible for the following:

(a) Ensuring that each common control complies with the requirements of MD 12.5.

(b) Ensuring all entities within their organization or under their control that are involved in acquiring (e.g., either developing or procuring) common controls comply with the NRC system development and security authorization requirements.

(c) Ensuring all implementations receive an authority to operate from the AO before being put into operation.

(d) Ensuring that required security documentation is prepared and maintained for each common control.

(e) Providing IT inventory information to OCIO for each common control that:

(i) Identifies all common control hardware, including model identification.

(ii) Identifies all software for each hardware component, including version identification.

(f) Performing continuous monitoring of common controls to determine if they are operating as intended and having the desired effect.

4. Security Control Assessor (SCA)

The security control assessor (SCA) is a trusted position with special access to the security posture of an IT system. The SCA is any individual, group, or organization responsible for conducting a comprehensive, independent assessment of the system cybersecurity controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The SCA is responsible for the following:

(a) Evaluating the system security plan before the system assessment is conducted to help ensure the plan provides a set of detailed security controls that is adequate to meet all applicable security requirements.

(b) Conducting a comprehensive assessment of the cybersecurity controls in an IT system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

(c) Providing a documented assessment of the severity of cybersecurity weaknesses or deficiencies discovered in the IT system.

(d) Recommending corrective actions to address identified vulnerabilities in the system.

(e) Preparing the final security assessment report containing the results and findings from the assessment.

5. Authorizing Official Designated Representative (AODR)

The Authorizing Official Designated Representatives (AODR) act on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated with the security authorization process. AODRs can be empowered by an AO to make certain decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the

assessment and/or determination of risk. They also may be called upon to prepare the final authorization package, obtain the AO signature on the authorization decision document, and transmit the authorization package to appropriate officials. The only activities that cannot be delegated to the AODR by the AO are the authorization decision and signing of the authorization decision document.

6. System-Level Information System Security Officer (ISSO)

   The system-level information system security officer (ISSO) is the designated security representative of an IT system owner. This is a trusted position with special access to and authority over an IT system. This role must not be assigned to an individual who has other trusted responsibilities (e.g., a system administrator should not be assigned ISSO responsibilities). The system-level ISSO has detailed knowledge and expertise required to manage the security aspects of the information systems, and may be assigned responsibility for the day-to-day security operations of the system. In some cases, however, due to staffing limitations or other constraints, it may be necessary to assign responsibilities of multiple trusted positions to a single individual. System owners must consult with the CISO before assigning ISSO responsibilities to an individual with other trusted responsibilities. The system-level ISSO is responsible for the following:

   (a) Overseeing the security aspects of the IT system and its day-to-day security operations.

   (b) Conveying system security information to OCIO/ISPO.

   (c) Identifying and correcting system cybersecurity issues.

   (d) Being responsible for one or more IT system(s).

7. Office Information System Security Officer (OISSO or office ISSO)

   The office information system security officer (OISSO or office ISSO) serves as the ISSO representative and single point of contact for ISSO responsibilities for one or more offices or regions, and communicates ISSO-relevant information to the rest of the office's system-level ISSOs and computer professionals. The OISSO is responsible for the following:

   (a) Conveying office-specific system security information to OCIO/ISPO. The office ISSO must be a system-level ISSO for at least one system within that office. The office ISSO has inherent U.S. Government authority and must be a Government employee.

   (b) Performing actions based upon information that cannot be provided to a system-level contractor ISSO due to homeland security and other information sensitivity restrictions and appropriately labeling the information as restricted from contractor access.

8. Information Security Architect (ISA)

   The information security architect (ISA) is responsible for ensuring that the enterprise architecture addresses cybersecurity requirements necessary to protect the agency's core missions and adequately addresses associated business processes. The ISA is responsible for the following:

   (a) Serving as the liaison between the enterprise architect and the information system security engineer.

   (b) Advising AOs, the CIO, and the CISO on a range of activities, including establishing system boundaries, assessing the severity of weaknesses and deficiencies in the system, plans of action and milestones (POA&M), risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

9. Information System Security Engineer (ISSE)

   The information system security engineer (ISSE) ensures incorporation of cybersecurity into systems from initiation of the system and throughout system changes. The ISSE is responsible for the following:

   (a) Defining system security requirements and associated verification methods.

   (b) Developing security aspects of the system architecture and design.

   (c) Identifying and assessing system vulnerabilities.

   (d) Proactively designing security functions.

   (e) Providing security considerations to inform systems engineering efforts with the objective to reduce errors, flaws, and weaknesses as well as address performance and effectiveness of cybersecurity control implementation.

   (f) Identifying, quantifying, and evaluating the costs and benefits of security functions and considerations to inform analysis of alternatives, engineering trade-offs, and risk decisions.

   (g) Performing system security analyses in support of decisionmaking, risk management, and engineering trade-offs.

10. NRC Authenticated Users

    An NRC authenticated user is an individual who has been authorized access to or use of an NRC IT system for any reason (e.g., support of an agency mission or developing or maintaining an IT system). For the purposes of MD 12.5, individuals in who only access NRC publicly available services for unauthenticated access are not considered to be NRC authenticated users.

    (a) NRC authenticated users must report all suspected attacks or other types of cybersecurity incidents within 1 hour of discovery to the CSIRT.

(b) NRC authenticated users shall not do the following:

(i) Connect to NRC networks or systems devices that have not been authorized as part of a system (e.g., desktops, servers, special purpose computers, wireless access points, printers, and video teleconferencing);

(ii) Use an Internet connection that bypasses the federally required Trusted Internet Connection (e.g., MyFi);

(iii) Connect personally owned devices (e.g., mobile phones, tablets, and thumb drives) to an NRC system (e.g., desktop, mobile desktop); and

(iv) Install software on NRC equipment that has not been authorized by the AO for use with the equipment.

(c) Users of an IT system are often the first to encounter an anomaly that may be indicative of an attack or actions associated with unauthorized execution of malicious program code. Thus, an IT system user community can serve as a control or countermeasure to identify potential attacks and mitigate the resulting adverse impacts through early recognition, reporting, and compliance with NRC security measures.

(d) Each NRC authenticated user must follow the "NRC Agency-wide Rules of Behavior for Authorized Computer Use" as well as any system-specific rules of behavior established by system owners. The rules of behavior are available on the OCIO Web site at http://www.internal.nrc.gov/CSO/documents/ROB.pdf. See Section IV for detailed information on cybersecurity rules of behavior.

11. Business Line Lead

A business line lead is an office director, a regional administrator, or a deputy executive director responsible for an NRC business line (e.g., nuclear reactor regulation). A business line lead has inherent Government authority, must be a Government employee, and is responsible for the following as it relates to cybersecurity:

(a) Identifying mission, business, and operational requirements and IT resources necessary for the business line to support the mission and for compliance with cybersecurity requirements.

(b) Identifying resources required for critical business processes, and determines the impact of unavailability of those resources.

(c) Performing a business line risk assessment.

(d) Developing a business continuity plan (BCP) for the business line.

C. External Parties

NRC must maintain the security of UUI, CUI, and classified information and information processing facilities with respect to parties external to the NRC. Risk must be identified and controls must be in place before access is granted to external parties.

1. Public Access to NRC IT Systems

   Some NRC IT systems include a public access component. These systems must include architecture and design strategies as well as specific access controls that minimize the potential for IT system and infrastructure compromises.

2. Visitors

   Personnel requiring access to IT systems and information processing facilities owned by NRC or operated on behalf of NRC must obtain access approval and follow visitor procedures as stated in MD 12.3, "NRC Personnel Security Program." Visitor access to NRC information processing facilities must be controlled by NRC-authorized personnel and must reflect cybersecurity controls identified in the system security plan(s) for systems located within the facility.

3. Cloud Computing and Hosted Solution Providers

   (a) Business capabilities are increasingly being met using less conventional contracting vehicles and external services. As a result, NRC capabilities may be hosted by another Federal agency or a third-party service provider. The hosting agency or provider must meet NRC cybersecurity requirements. All organizations contracted to host a shared service or provide a cloud-based computing capability must have a system security Terms of Service Agreement with another Federal agency that applies to the NRC, or a system security Terms of Service Agreement with the NRC.

   (b) Use of shared systems and environments introduces shared risks, vulnerabilities, and exposures, and untrusted parties may have access to the same shared resources. All risks must be carefully considered, and then mitigated or accepted before using cloud computing and hosted solution providers.

4. IT Contracts

   (a) All NRC IT-related contracts shall include cybersecurity requirements identifying the personnel security and system security requirements for the prime contractor and any subcontractors including, but not limited to, contractor background checks and access approval clauses. New requirements may be added, which may include the development and maintenance of security documentation and system vulnerability scans, as appropriate. All contracts shall include the following:

      (i) The requirement to allow for the vulnerability scanning of systems, security documentation, and contractor background checks;

      (ii) The requirement to comply with MD 12.5; and

      (iii) Contractor staff must maintain the requisite role-based cybersecurity training at the contractor's expense.

   (b) All contractors that use NRC computing resources must assume the same responsibilities as NRC staff as defined in MD 12.5.

5. Interagency Agreements

   All NRC IT-related interagency agreements must be approved by the CIO and shall include cybersecurity requirements for connections to NRC systems in the form of Interconnection Security Agreements. The template for the Interconnection Security Agreement can be found at http://www.internal.nrc.gov/CSO/security_templates.html.

6. Foreign Assignees

   Foreign assignees that are assigned at the NRC must have a CISO and ADM/DFS-approved security plan that clearly defines cybersecurity requirements that apply to their NRC efforts. The office sponsoring the foreign assignee must submit this plan to the CISO and ADM/DFS for approval. This plan must be approved by the CISO and ADM/DFS before the foreign assignee is given access to NRC computing capabilities. Foreign assignees must obtain access approval, follow the security plan, and follow procedures as stated in MD 12.1, "NRC Facility Security Program."

7. System Interconnections within NRC

   Connections between NRC IT systems that involve multiple system owners must be approved during the authorization process. Once approved, system owners are responsible for ensuring that the agreed upon set of security controls that govern these connections are maintained. The template for the Interconnection Security Agreement can be found at http://www.internal.nrc.gov/CSO/security_templates.html.

8. System Interconnections with External Systems

   All connections and agreements related to connections between an NRC IT system and another Federal agency system or a system owned by another party must be approved during the authorization process and signed by the CIO. Once approved, system owners are responsible for ensuring that the agreed upon set of security controls that govern these connections are maintained.

III. INFORMATION TECHNOLOGY ASSET MANAGEMENT

A. NRC Assets

1. An asset is anything that has value to the NRC. MD 13.1, "Property Management," provides the definition of NRC property and identifies requirements for management of NRC property. The official NRC IT asset inventory is maintained by OCIO. The IT asset inventory identifies all hardware and software that belongs to a specific system and serves to meet the FISMA requirement for a system inventory.

2. NRC IT assets (e.g., hardware, software) vary greatly in purpose, use, complexity, sensitivity, criticality, and importance to the agency. Applying equal levels of security, management, resources, and control to all assets is not possible or cost-effective. Effective management of IT assets is performed based upon the value of the asset to NRC and asset characteristics. All assets that process, store, or transmit NRC information for or on behalf of NRC must be a part of a system that is identified in the IT system inventory.

3. OCIO shall maintain a current and authoritative IT system inventory. If the information in the inventory is classified, then that part of the inventory shall be maintained in a classified system. Information within the inventory shall only be added, modified, or deleted by the information owner or designee. Where possible, information shall be captured from an automated inventory capability and used to populate the inventory information fields

B. Information Classification

1. IT systems are categorized based upon the sensitivity of information processed by the system and upon the intended purpose of the system. Information used within NRC falls within these major categories: UUI, classified information, and CUI. MD 12.3, along with an individual's job requirements and need to know, govern the individual authority to access information. OIG, in accordance with the Inspector General (IG) Act of 1978 (5 U.S.C. App 3), is authorized access to agency information for the purpose of carrying out the OIG audit and investigative functions.

2. All IT systems must be categorized at the highest level of sensitivity of any information processed, stored, or transmitted by the system using OCIO-CS-PROS-2001, "System Security Categorization Process." This concept is referred to as "system high" categorization. System high mode is distinguished from other modes (including multilevel security) by the lack of trust of the host IT system to separate classifications. As a result, all information in a system high IT system is treated as if it were classified at the highest security level of any data in the system. For example, unclassified information can exist in a secret system high computer, but the information must be treated as secret, and cannot therefore be declassified while it remains on the system. Electronic output must be manually reviewed and approved before the classification level can be changed.

3. Any information pertaining to the security posture of an IT system must be protected at the level of the system to which it applies.

4. Any information that reveals techniques used within an IT system, the knowledge of which may enable a malicious user to exploit the system, must be protected at the level of the system to which it applies.

5. Automated declassification of information introduces a serious risk of system exploitation and is therefore not allowed within NRC.

C. Classified Information

1. Information is determined to be classified information by a trained and authorized original or derivative classifier (defined in MD 12.2, "NRC Classified Information Security Program"). MD 12.2 provides direction for appropriate classification and non-IT handling of classified information. IT processing, storage, and transmission of classified information must follow CNSS direction and MD 12.5. IT processing, storage, and transmission of classified information at the SCI level must follow DNI policy, standards,

and guidance and MD 12.5. Classified information may NOT be processed, transmitted, or stored on an unclassified system or network. Classified information must only be stored, processed, or transmitted using systems that have been provided an NRC authority to operate for classified information processing.

2. The program used to protect classified information is Communications Security (COMSEC). The term COMSEC material, as used in this handbook, includes items designed to secure or authenticate telecommunications of national security information. COMSEC material includes, but is not limited to, keys, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items used to perform COMSEC functions. MD 12.4, "NRC Communications Security (COMSEC) Program," provides additional NRC policy for COMSEC.

D. Controlled Unclassified Information (CUI)

1. CUI is information that is not classified; however, a compromise of the confidentiality, integrity, or availability of the information could cause an adverse effect on NRC operations, NRC assets, or individuals.

2. Systems processing CUI must have a FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," confidentiality sensitivity of at least moderate.

3. IT processing, storage, and transmission of CUI must follow MD 12.5.

E. Controlled Unclassified Information (CUI) Specified

1. General

   CUI Specified is the subset of CUI in which the authorizing law, regulation, or Governmentwide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Governmentwide policies include such specific requirements. The CUI Registry is available at https://www.archives.gov/cui. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority provides specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Governmentwide policies do not provide specific guidance. IT processing, storage, and transmission of CUI must follow MD 12.5.

2. Controlled Unclassified Information Specified Safeguards Information (CUI/SP-SGI)

   (a) Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material or security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities must be protected pursuant to Section 147 of the Atomic Energy Act (AEA) of 1954, as amended (42 U.S.C. 2011 et seq.), is referred to as CUI Specified

Safeguards information (CUI/SP-SGI). CUI/SP-SGI must be protected, and unauthorized disclosures of CUI/SP-SGI are subject to civil and criminal sanctions.

(b) Information is designated to be CUI/SP-SGI by certified SGI designators. MD 12.7, "NRC Safeguards Information Security Program," provides direction for appropriate designation and non-IT handling of CUI/SP-SGI. IT processing, storage, and disposal of CUI/SP-SGI must follow MD 12.5. CUI/SP-SGI shall NOT be processed, transmitted, or stored on an IT system or network that has not been approved by the NRC AO for CUI/SP-SGI processing.

3. Controlled Unclassified Information Specified that is not CUI/SP-SGI (CUI/SP non-SGI)

   CUI Specified non-SGI refers to all CUI Specified information other than CUI Specified SGI.

4. Controlled Unclassified Information Basic

   CUI Basic is the subset of CUI for which the authorizing law, regulation, or Governmentwide policy does not set out specific handling or dissemination controls. CUI Basic is handled according to the uniform set of controls set forth by CUI. CUI Basic differs from CUI Specified, and CUI Basic controls apply whenever CUI Specified controls do not cover the involved CUI.

F. Uncontrolled Unclassified Information (UUI)

1. UUI is information that is not sensitive with respect to confidentiality; however, a compromise of the integrity or availability of the information could cause an adverse effect on NRC operations, NRC assets, or individuals.

2. IT processing, storage, and transmission of UUI must follow MD 12.5.

3. Systems processing UUI must comply with the minimum NIST SP 800-53 baseline set of controls.

G. Asset Accountability and Ownership

The purpose of IT assets is to support the NRC mission and objectives. All IT assets shall be identified and have a responsible owner. Asset owners do not have to be IT system owners or information owners. An asset owner is an individual or entity that has been assigned responsibility by management for controlling the production, development, maintenance, use, or security of an IT asset. Asset owners shall establish and maintain the security controls necessary to provide protection for IT assets. Asset accountability is important to help control costs, ensure that threats to NRC assets are correctly identified, and ensure adherence to licensing restrictions. NRC authenticated users shall not use NRC IT assets for any non-Government activity, except in accordance with the NRC limited personal use policy (see MD 2.7, "Personal Use of Information Technology").

H. Asset Refresh

IT assets must be under general vendor support and must be able to meet NRC processing requirements. Any hardware or software asset that is out of general vendor support (special support must be contracted) must be refreshed (replaced with a supported asset). Any hardware that cannot run the current NRC required software versions with current patches for software must be refreshed to hardware that can run them. Any software that cannot run the current NRC-required versions with current patches for other software must be refreshed to software that can run them.

IV. PERSONNEL

This section discusses staff responsibilities for cybersecurity.

A. Personnel Screening

1. MD 12.3 provides information on the pre-employment screening of NRC applicants and contractors, national security clearance processing, visitor requirements, foreign nationals, and individual information and facility/system access authorizations.

2. NRC management shall assign a risk designation to all positions, establish screening criteria for individuals filling those positions, and annually review and revise position risk designations. NRC shall screen individuals before authorizing access to the IT system in accordance with CSO-STD-0020, “Organization Defined Values for System Security Controls.” This standard is available at http://www.internal.nrc.gov/CSO/standards.html.

B. Cybersecurity Rules of Behavior

1. Federal directives require agencies to establish rules of behavior for individual users to govern the secure use of IT resources. The NRC rules of behavior for all users are called the “NRC Agency-wide Rules of Behavior for Authorized Computer Use” (available on the http://www.internal.nrc.gov/CSO/ and are referred to in this document as the “rules of behavior”). The rules of behavior specify user-level rules for the secure use of all IT resources used to process or store UUI, CUI, or classified information. Each NRC authenticated user must follow the rules of behavior and sign the acknowledgement statement to indicate an understanding and acceptance of the rules of behavior before gaining access to any system that processes UUI, CUI, or classified information, whether at the primary workplace, an alternative workplace (e.g., teleworking from home or from a satellite site), or on official travel.

2. CSO-STD-0020 provides information on the frequency of acknowledgement, review, and update of rules of behavior.

3. Office directors and regional administrators are responsible for ensuring that all users acknowledge the rules of behavior in accordance with the frequency defined in CSO-STD-0020.

4. Individual systems may require separate acknowledgement of additional rules depending on the nature of the system and of the information processed by that system. For these systems, users are required to acknowledge that they will abide by

system-specific rules of behavior in addition to the agency rules of behavior as a condition of gaining and retaining access to the system.

5. If an individual violates or observes a violation of the rules of behavior, he or she must report the violation to the CSIRT, the violating user's management or project officer, and system ISSO.

C. Cybersecurity Awareness, Training, and Education

1. Objective

   The objective of NRC cybersecurity awareness, training, and education is to develop and maintain an NRC IT security workforce and NRC staff with a common understanding of the concepts, principles, and applications of cybersecurity to enhance the confidentiality, integrity, and availability of NRC's IT systems and IT resources.

2. New NRC Employees and Authenticated Users

   All new NRC employees shall receive an initial cybersecurity awareness briefing. All NRC authenticated users are required to take the annual cybersecurity awareness course within 1 week of obtaining access to NRC electronic information and annually thereafter.

3. Office Directors and Regional Administrators

   (a) Office directors and regional administrators shall ensure that all individuals with significant IT security responsibilities receive cybersecurity training in accordance with the NRC IT Security Role-based Training Plan available from the OCIO cybersecurity Web site at http://www.internal.nrc.gov/CSO/. Training requirements for individuals with classified system responsibilities are defined by the CNSS.

   (b) Office directors and regional administrators are responsible for tracking and reporting to the CISO and to the Office of the Chief Human Capital Officer (OCHCO) the requisite role-based IT security training received by those identified with significant IT security responsibilities.

   (c) Office directors and regional administrators shall ensure that staff cybersecurity training activities are recorded, monitored, and retained in accordance with MDs in Vol. 3, "Information Management," Part 2, "Records Management."

4. Employees and Contractors with Assigned Security and Privacy Roles and Responsibilities

   In compliance with OMB policy, employees and contractors with assigned security and privacy roles and responsibilities (e.g., ISSOs, System Administrators) must complete required role-based training before assuming the role. NRC contractors must ensure that their staff receives the requisite role-based cybersecurity training at the contractor's expense.

D. Consequences of Non-Compliance

1. Failure to comply with MD 12.5 may result in action including but not limited to the following:

   (a) Removal of system access for a specific period of time,

   (b) Discipline up to and including removal from the Federal service, and

   (c) Prosecution under applicable law.

2. Allegations of violation must be reported to the OIG.

E. Termination or Change of Employment

As duties and responsibilities of IT users change, cybersecurity controls and information access rights associated with the individual are changed accordingly.

1. Associate Director for Human Resources Operations and Policy, OCHCO

   (a) The Associate Director for Human Resources Operations and Policy shall notify system owners of expected NRC staff terminations and transfers, and changes as specified in CSO-STD-0020. For terminations, a notification shall indicate whether or not the termination is voluntary.

   (b) The Associate Director for Human Resources Operations and Policy shall notify system owners of unexpected NRC staff terminations, transfers, and changes immediately. For terminations, a notification shall indicate whether or not the termination is voluntary.

2. System Owners

   (a) System owners, in coordination with information owners, shall review with exiting personnel the information they can and cannot share with others.

   (b) System owners shall ensure an exit interview is conducted with employees whose employment is terminated to obtain important system information from the employee and to ensure access to information and IT systems is not disrupted.

   (c) System owners shall ensure the return of all IT system-related property (e.g., keys, identification cards, mobile devices), and ensure that appropriate personnel have access to official records created by the transferring or terminated employee that are stored on organizational IT systems.

   (d) System owners shall ensure the continued availability of information and IT systems upon employee or contractor termination.

   (e) System owners shall ensure that departing personnel records of physical access, system user accounts, application and information access data, the identity of hardware and software assets that were individually “owned” or used by the individual (non-privileged), and privileged accounts are retained in accordance with CSO-STD-0020. This ensures that historical information will be available as needed.

V. PHYSICAL AND ENVIRONMENTAL SECURITY

Physical and environmental security protects facilities, equipment, and information from damage and compromise. This section describes physical and environmental security functions within the NRC that are required to ensure that IT assets are physically protected from damage, theft, or physical invasion that could result in compromise of UUI, CUI, or classified information.

A. Secure Areas

1. Facility physical security is the responsibility of the Office of Administration (ADM) Division of Facilities and Security (DFS also ADM/DFS), and overall NRC facility physical security policy is provided in MD 12.1, “NRC Facility Security Program.” MD 12.1 also identifies physical security requirements for non-NRC facilities that handle UUI, CUI, or classified information. MD 12.1 does not address requirements for electronic processing of UUI, CUI, or classified information.
2. The NRC AO must approve facilities for non-public information processing before use of the facilities for this purpose. The facility must meet all facility-level cybersecurity requirements for non-public information processing.
3. In addition to the requirements for facility physical security as outlined in MD 12.1, external facility doors and windows to locations housing NRC computers or computers that process, store, or transmit NRC non-public electronic information must be locked when unattended. External protection also is required for windows, particularly at ground level.
4. Access to secure areas where non-public information is processed or stored must be controlled and restricted to authorized persons only. Authentication controls, including access control cards, must be used to authorize and validate access to those areas. ADM/DFS must maintain a secure audit trail of access, using the Personal Identity Verification (PIV) card. See MD 12.1 for PIV card access requirements and information on Homeland Security Presidential Directive 12 (HSPD-12).

B. Equipment Security

1. NRC equipment must be protected from physical and environmental threats so as to prevent loss, damage, theft, or compromise of IT assets and interruption to the organization’s activities.
2. Protection of IT equipment, including equipment that is offsite, unused, or in disposal, is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage.
3. IT equipment must be cleaned of all information using approved data wiping tools before the resource is decommissioned or re-purposed for another use. Only data wiping tools approved by the CISO and the CIO can be used.

VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT

A. Overview

UUI, CUI, and classified information shall only be processed, stored, or transmitted on equipment using an AO-approved business solution, including the approved use of personally owned devices that are NRC-configured.

B. Requirements for Approved Systems or Business Solutions

The following are requirements for AO-approved systems or business solutions:

1. Classified System Connectivity

   (a) Classified systems must only connect to classified systems operating at the same classification level, except where using approved encrypted connections that permit transmission over lower level networks.

   (b) Classified systems must only connect to other systems using techniques and capabilities specifically approved by the AO for connecting to the classified system.

2. CUI/SP-SGI System Connectivity

   (a) CUI/SP-SGI systems must only connect to other CUI/SP-SGI systems, except where using approved encrypted connections that permit transmission over lower level networks.

   (b) CUI/SP-SGI laptops must only connect to CUI/SP-SGI systems using techniques and capabilities specifically approved by the AO for connecting to the CUI/SP-SGI system.

3. NRC User Information Access

   (a) Users shall only download or store CUI to the hard drive of a computer or other media that is approved by NRC for information storage of the category/subcategory of information. This includes computers provided at teleworking centers.

   (b) Users shall only process UUI and CUI on NRC computers approved for processing of the specific category/subcategory of information, even when the storage media is a floppy disk, CD, DVD, thumb drive, or any other external media. Employees who work at home or at approved telework locations must perform electronic processing of UUI or CUI that is not CUI/SP-SGI on either—

      (i) A personally owned computer or provided telework location computer using a business solution approved for this use (e.g., a Citrix connection where actual processing is occurring on the Citrix server rather than the personal owned computer or NRC-provided telework location computer), or

      (ii) An NRC-issued computer that is compliant with the NRC requirements.

C. Operational Procedures and Responsibilities

1. General

   (a) NRC requires standard operating procedures for similar IT platforms located across NRC business organizations to ensure that security settings or features are uniformly applied. A central change management board shall be responsible for approving and managing changes to system procedures across the enterprise. Moreover, system owners must document procedures and configurations to help the board appropriately handle system interdependencies. System operating procedures and configurations are formal documentation and official agency records.

   (b) When outside of a facility that has been approved for IT processing by the AO, system owners shall ensure encryption of electronic CUI and classified information in accordance with OCIO-CS-STD-2009, "Cryptographic Control Standard."

2. Documented Operating Procedures

   (a) System owners shall ensure operating procedures for processes that support the secure operation of their IT systems are developed, documented, maintained, and made available upon request to users in need of these procedures. At a minimum, system owners shall ensure development of system-specific operating procedures for each IT system and facility that meet CSO-STD-2001, "System Documented Operating Procedures," which is available from the OCIO Cybersecurity Standards Web site at http://www.internal.nrc.gov/CSO/standards.html.

   (b) Other operating procedures for significant IT system and facility activities shall be developed as necessary. If the failure or malfunction of an IT system could greatly impact execution of the NRC mission, the system is considered a significant IT system.

3. Separation of Duties

   (a) Separation of duties is a key internal control concept that reduces the opportunity for unauthorized or unintentional modification or misuse of NRC IT system resources or data. Separation of duties is achieved by distributing privileges to complete an activity across multiple individuals serving in different roles so that more than one person is required to complete significant tasks. Four different types of activities require separation of duties:

      (i) Authorization. User activities that involve the review and approval of transactions or operations. For example, authorization processes for IT systems include approving change requests, IT system design, or programming changes.

      (ii) Custody. User activities that involve the physical control of an asset. An asset's custodian is not necessarily responsible for maintaining records relating to the asset.

(iii) Recordkeeping. User activities that create and maintain transaction information.

(iv) Reconciliation. User activities that verify transactions to ensure that the transactions are valid, authorized, and recorded in a timely manner and on a regular basis.

(b) No one person should perform more than one of these activities.

(c) If a single person is able to hide malicious behavior or inappropriate use of resources using his or her authority, separation of duties has not been exercised.

4. Separation of Development, Test, and Operational Environments

(a) General

Three different environments (development, test, and operational) are used to implement and deploy IT systems. These environments shall be physically or logically independent of each other. Security controls shall be put in place to ensure that these environments cannot be accessed from one another except through AO-authorized mechanisms.

(b) Development, Test, and Operational Environments

(i) Firewalls, access control lists, boundary routers, etc., shall be employed to ensure that all NRC IT environments (including those operated for or on behalf of NRC) are properly separated. System owners must ensure each environment is protected at the level of sensitivity of the information stored, accessed, or processed within that environment.

(c) Development Environment

(i) This is the environment in which a system is created. Developers have significant privileges on the development systems they used to create and integrate software and hardware capabilities. The primary form of control associated with the development environment is a configuration management (CM) system that is used to control access to code and track changes to the code.

(ii) System owners shall ensure development activities are performed only within the development environment and are not performed within the test or operational environment.

(d) Test Environment

(i) This is the environment in which each system release is tested before being placed into an operational environment.

(ii) System owners shall ensure only test information/dummy data is used within the test environment wherever technically and operationally feasible. If system owners cannot use test information/dummy data, they shall enforce the same information access restrictions on the test environment as they

enforce in the operational environment. Interface testing with other systems is performed in the test environment.

(iii) System owners shall ensure release testing occurs within the test environment.

(iv) Releases from the test environment to the operational environment shall follow established, agencywide CM processes and procedures.

(e) Operational Environment

This is the environment in which mission functions are performed. This environment is stable and requires AO authorization before this environment is modified. Performing testing or development on operational networks or within operational environments increase the risk for data corruption, modification, and introduction of false data into the operational environment and is not permitted without AO authorization. All tools installed or used within the operational environment must be approved by the AO. System owners are encouraged to identify and obtain approval for tools in advance of planned use.

5. Security of System Documentation

(a) System documentation contains details that can be used to exploit the system. In addition, unauthorized modification to system documentation can result in inappropriate action that could enable system destruction or compromise.

(b) System owners shall ensure access to system documentation is controlled to protect against unauthorized access.

6. Copying, Scanning, Printing, and Faxing

(a) Only approved copiers, scanners, printers, and fax machines may be purchased by the NRC. These devices are analyzed and assessed for potential cybersecurity risks. Only those devices that do not pose an undue risk are approved. The information needed for these assessments shall include but will not be limited to the following: the exact device to be purchased, the intended use of the device, and the device's capabilities.

(b) Top Secret information shall not be copied or reproduced without approval from the Top Secret Control Officer (defined in MD 12.2).

(c) Copiers, scanners, printers, and fax machines that are connected to an unclassified, non-safeguards information (non-CUI/SP-SGI) network shall not be used for either CUI/SP-SGI or classified information.

(d) Copiers, scanners, printers, and fax machines that are connected to a CUI/SP-SGI network and reside in an ADM/DFS-approved space may be used for CUI/SP-SGI. Printers must have a banner or separation page either (1) before or after each print job or (2) a blank page printed at the end of the print job. Each machine shall be labeled as a CUI/SP-SGI device and located in an ADM/DFS-approved space.

(e) Copiers, scanners, printers, and fax machines that are connected to a classified network may be used for classified information at the level of the network. Printers must have a banner or separation page either (1) before or after each print job or (2) a blank page printed at the end of the print job. Each machine shall be labeled to match the level of classified processing. Copier output shall be handled consistent with the markings on the original and should be considered classified until verified by an Authorized Derivative Classifier or Authorized Original Classifier (defined in MD 12.2).

(f) Copiers that are not connected to a network and do not have disk storage may be used for multi-level processing as long as the operating procedures for use of the copier for the level of the computer or network are followed. Printers must have a banner page before each print job indicating the classification level of the print job. The copier shall be labeled for multi-level processing and the procedures for each level of processing shall be posted in clear view at the copier.

(g) Copiers that are not connected to a network that have disk storage or persistent memory may be used for multi-level processing as long as there is a CISO-approved method of wiping the disk storage and persistent memory and the operating procedures for use of the copier for the level of the computer or network are followed. Printers must have a banner page before each print job indicating the classification level of the print job. The copier shall be labeled for multi-level processing and the procedures for each level of processing shall be posted in clear view at the copier.

(h) Copying, scanning, printing, and faxing of CUI/SP-SGI and classified information require constant monitoring by an individual properly authorized for access to the information, and the machines shall be continuously attended by a properly authorized individual until completion of the process.

(i) All extra copies and waste must be treated at the same level as the information being processed.

(j) Printers without disk storage and without persistent memory may be used for multi-level processing. The printer may be directly attached to a computer or network operating at the CUI/SP-SGI or classified level as long as the operating procedures for use of the printer for the level of the computer or network are followed. Printers must have a banner page before each print job indicating the classification level of the print job. The printer shall be labeled for multi-level processing and the procedures for each level of processing shall be attached to the printer.

(k) Printers with disk storage or persistent memory may be used for multi-level processing if there is an authorized capability to erase both the disk storage and persistent memory between print jobs. Detailed directions on use of the erase procedure must be attached to the printer, and users must sign a rules of behavior for multilevel printing on the device. Printers must have a banner page

before each print job indicating the classification level of the print job. The printer shall be labeled for multi-level processing and the requirements posted.

D. Security-Focused Configuration Management and Change Control (SecCM)

Security-Focused Configuration Management and Change Control (SecCM) involves managing and controlling secure system configurations to facilitate the management of risk and is required for all NRC systems. SecCM consists of the following four phases:

1. Planning: Planning involves incorporating SecCM into policy and procedures and ensuring they address at least the following:
   (a) Implementation of SecCM plans;
   (b) Integration of SecCM into existing security program plans, Configuration Control Boards (CCBs), configuration change control processes, and tools and technology.
   (c) Use of common secure configurations and baseline configurations.
   (d) Monitoring metrics for compliance with established SecCM policy and procedures.
2. Identifying and implementing configurations: This phase includes the following:
   (a) Developing, approving, and implementing a secure baseline configuration that represents the most secure state consistent with operational requirements and constraints for the system.
   (b) Automation is used where possible to enable interoperability of tools and uniformity of baseline configurations across the system.
3. Controlling configuration changes: This phase includes the following:
   (a) Managing change to maintain the secure, approved baseline of the information system.
   (b) Ensuring that changes are formally identified, analyzed for security impact, tested, and approved prior to implementation.
4. Monitoring: This phase includes the following:
   (a) Validating that the approved secure baseline configuration is in place and operating as intended.
   (b) Identifying undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes.
   (c) Using automated tools where possible.

E. Third-Party Service Delivery Management

1. Security

   Security is a critical component of third-party services. System owners are ultimately responsible for the security of information processed by a third party. The agreement between the NRC and the third party shall—

   (a) Provide guidance for the implementation and maintenance of cybersecurity controls when NRC IT owners use third-party services.

   (b) Define the service that is being provided, describe how the service will be monitored and reviewed, and specify the ways the service can be modified if both parties agree.

   (c) Ensure proper escort and oversight of maintenance personnel that service NRC IT equipment.

2. System Owners

   System owners shall ensure that the services, reports, and records provided by the third party are regularly monitored and reviewed. System owners shall conduct periodic (at least annual) assessments and ensure the service provider adheres to the cybersecurity terms and conditions of the agreements, properly manages cybersecurity incidents, and adequately addresses all deficiencies.

3. Requirements

   Specific cybersecurity requirements on securing third-party services can be found at the OCIO cybersecurity Web site at http://www.internal.nrc.gov/CSO/.

F. System Planning and Acceptance

1. System owners shall ensure that effective system planning and acceptance processes are followed to minimize the risk of system failure or service interruption. Advance planning and preparation is required to ensure that NRC IT systems meet business requirements and comply with requirements to protect confidentiality, ensure system and data integrity, and provide resource capacity to ensure availability. System owners shall ensure that any risks to their IT systems are properly managed.

2. System owners shall ensure non-NRC facilities hosting NRC IT systems meet federally mandated and NRC-defined security requirements, and this information shall be incorporated in system security documentation.

3. IT system security controls shall be included in the initial planning phase of system development. System owners must verify implementation of controls before system acceptance.

4. All connections between NRC IT systems owned by different system owners must be approved by the respective system owner and interconnection agreements must be signed by the system owners.

5. All systems must obtain a security ATO before being placed into the operational environment. All IT resources must belong to an NRC IT system, and must therefore be part of a system ATO before being placed into operation. This includes all new systems and major modifications to existing systems. To maintain a system authorization all systems must adhere to specified ATO conditions and maintain a continuous monitoring program that provides the following:

   (a) Addresses effectiveness of deployed security controls,

   (b) Addresses changes to IT systems and the environments in which those systems operate (through formal security impact analyses), and

   (c) Complies with Federal legislation, directives, policies, standards, and guidance with regard to cybersecurity and risk management.

6. System owners shall ensure a national security system determination is made using NIST Special Publications (SP) 800-59, "Guideline for Identifying an Information System as a National Security System" (available from the NIST Web site at http://csrc.nist.gov/publications/PubsSPs.html) before performing any other system actions.

7. The intelligence community retains authority for all systems that process sensitive compartmented information and their policies, directives, and instructions shall be used for those systems.

8. CNSS policies, directives, and instructions, available from the CNSS Web site at http://www.cnss.gov/, shall be used for all other classified systems.

9. When NRC uses a system owned by another agency that processes classified information and does not follow CNSS policies, directives, and instructions, the NRC AO shall determine if the implemented controls are sufficient to accept the risk of using the system.

G. Protection Against Malicious and Mobile Code

1. NRC Authenticated User Responsibilities

   NRC authenticated users must be cognizant of their responsibilities for applying protective measures to prevent the introduction of potentially damaging software into the NRC infrastructure. Protection mechanisms against malicious and mobile code require multiple protection mechanisms at the network, operating system, and application layers. These protection mechanisms must detect and repair effects of undetected malicious and mobile code. Protection includes educating users on the dangers of malicious code. Malicious and mobile code, in combination with social engineering techniques, can successfully target the user community because they receive the least amount of technical training and are most likely to be targeted by attackers.

2. Malicious Code

   (a) Protection

   Protection against malicious code is a multi-pronged defense, involving prevention, detection, and recovery. System owners shall ensure that protections employed against malicious code adhere to all federally mandated requirements, NRC-defined security requirements, and organizationally defined values. First, technical controls are employed to prevent malicious code from entering NRC networks and systems. Second, technical controls are used to detect and repair malicious code that manages to get past the first set of controls. Next, continuing education and awareness are used to remind users of threats to NRC assets. Last, comprehensive procedures are employed for access and change management.

   (b) NRC IT systems shall employ malicious code protection mechanisms as follows:

      (i) At IT system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;

      (ii) For electronic mail, electronic mail attachments, Web accesses, removable media, or other public Internet access mechanisms;

      (iii) To protect against malicious code inserted through the exploitation of a system's vulnerabilities;

      (iv) To protect against malicious code that may be resident on media and devices connected to an NRC IT system; and

      (v) To allow only AO-approved active electronic media to be used with NRC equipment.

3. Mobile Code

   (a) Mobile code is software that transfers from one computer to another and then executes automatically to perform a specific function with little or no user interaction.

   (b) System owners shall ensure that only authorized implementations of mobile code are used in their systems.

4. Peer-to-Peer Software

   The installation of Peer-to-Peer (P2P) capability on NRC computers without explicit written approval of the NRC AO is strictly prohibited.

H. Data Backup

System owners shall ensure their system backup strategy provides data confidentiality, integrity, and availability (C-I-A) after a local system failure or site disaster. System owners are ultimately responsible for ensuring that restored backups provide C-I-A, even when service providers execute the backups.

I. Classified Telecommunication

1. Communications Security (COMSEC)

   (a) COMSEC is a component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of telecommunications, while information is transmitted by telephone, cable, microwave, satellite, or any other means. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. COMSEC information is considered especially sensitive because of the need to safeguard U.S. cryptographic principles, methods, and material against exploitation.

   (b) Because of the extremely sensitive nature of COMSEC, managers must obtain prior approval from the Central Office of Record (COR) (a position held by a member of the Office of Nuclear Security and Incident Response (NSIR), Division of Security Operations (DSO), Information Security Branch (ISB)) for the release of operational COMSEC materials. Managers and Information System Security Officers shall ensure that their personnel follow up with the COR on any security deficiencies involving COMSEC or classified telecommunications systems and ensure mitigation in accordance with COR direction. Detailed requirements regarding COMSEC can be found in MD 12.4.

2. Transmission and Emanations Security

   (a) Transmission security (TRANSEC) measures security controls applied to transmissions to prevent interception, disruption of reception, communications deception, and derivation of intelligence by analysis of transmission characteristics including signal parameters or message externals. TRANSEC is that field of COMSEC that deals with the security of communication transmissions, rather than that of the information being communicated.

   (b) To accomplish TRANSEC, the NRC has separation requirements in place to ensure classified information cannot be inadvertently transferred to unclassified transmission media and equipment. The RED/BLACK concept refers to the careful segregation in cryptographic systems of signals that contain classified plaintext information (RED signals) from those that carry encrypted information, or cipher text (BLACK signals). Red/black separation requires shielded cabling, system isolation to cleared spaces, the use of cryptographic equipment, and technical surveillance countermeasures.

   (c) Any classified system must be designed and installed within NRC security-controlled areas. Contact the Chief, Facilities Security Branch (FSB), DFS, ADM, for additional information regarding NRC-controlled areas. Additional information regarding technical surveillance countermeasures inspections can be found in MD 12.1.

(d) Emanations Security is protection that results from measures taken to deny unauthorized individuals access to information derived from intercept and analysis of compromising emissions from crypto-equipment or an information system. All electronic equipment—including microcomputers, typewriters, printers, scanners, monitors, and network cabling—emit electrical and electromagnetic radiation through the air or through conductors. The possibility exists that electronic eavesdroppers could intercept emanations, decipher them, and use this information to reconstruct the data being processed by the equipment, even if the eavesdropper is located some distance from the equipment. The use of TEMPEST-certified technology is the preferred method of protecting against compromising emanations.

(e) TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations from telecommunications and automated information systems equipment. Compromising emanations are unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information system equipment. Under certain circumstances and in some specific physical environments, non-TEMPEST telecommunications equipment may be used to communicate classified information when the COR approves this in writing.

(f) The use of equipment in an unshielded environment must be determined on a case-by-case basis in the normal process of developing a physical security plan. ADM/DFS will, upon request, arrange for technical security inspections (e.g., TEMPEST) or countermeasures inspections of secure telecommunications systems or facilities as dictated by local conditions or circumstances. See MD 12.1 for additional information.

3. Secure Facsimile

   All classified and sensitive unclassified information telecommunicated by facsimile must be transmitted over protected systems. Contact the COR for additional information.

J. Voice Telecommunications

1. Classified information and CUI/SP-SGI voice telecommunications, whether by telephone, radio, video teleconferencing, or another means, shall be transmitted over protected systems to the maximum degree possible. Secure telephones controlled by NSIR/DSO/ISB are the NRC-preferred telephone for voice transmission of classified information and CUI/SP-SGI. Requests for secure telephones must be submitted in writing to the COR. Resident inspectors requesting secure voice capability should submit the request through the regional COMSEC manager for concurrence. Requests for other secure telecommunications equipment should be submitted to the COR.

2. The location of the secure telephone must be confirmed visually each working day or upon opening of the room where the telephone is located. The survey must include looking for signs of tampering and physical or cryptographic insecurities. Loss or

possible compromise of the secure telephone must be reported to the COMSEC Manager immediately (within 1 hour), who then must report it to the NRC COR. The COMSEC Account Manager must verify continued possession during the semi-annual inventory process at a minimum, by physically sighting and maintaining a written record of the secure telephone. The secure telephone must reside in an ADM/DFS-approved space and must have an ADM/DFS-approved security plan. Material held at a distant location (i.e., users located 25 or more miles from the account) that could not be sighted by the COMSEC Account Manager during an inventory requires that a new hand receipt be issued. When this occurs, the COMSEC Account Manager of the issuing COMSEC Account must generate a new hand receipt for signature by the distant location hand receipt holder during the semi-annual inventory process. The cryptographic keycard (KSV-21) for the secure telephone is a controlled cryptographic item (CCI) and must be protected in accordance with CNSS Instruction 4001, "(U) Controlled Cryptographic Items," May 2013. When CCIs contain keying material, protective measures must be consistent with the highest classification of the keying material, its purpose, and the sensitivity of the information or function being protected by the keying material.

3. Any relocation of a secure telephone, whether temporary or permanent, must be approved by the cognizant COMSEC manager. If a secure telephone is no longer required, contact the COMSEC manager for disposition instructions. All COMSEC incidents related to the loss, compromise, or possible compromise of secure phone equipment or keys must be reported immediately by secure means to the NRC COR.
4. Questions about NRC key management should be directed to the appropriate COMSEC manager or the NRC COR.
5. COMSEC managers shall perform semi-annual inventories and issue hand-receipts to holders of COMSEC equipment.
6. Secure phone users are responsible for the proper use and control of their phones and authentication media (e.g., keycard). Secure phone users shall perform the following:
   (a) Use the secure telephone only in a space approved by ADM/DFS.
   (b) Adhere to the security plan approved by ADM/DFS for the approved space.
   (c) Use the secure mode when discussing classified information or CUI/SP-SGI.
   (d) Close the door to the room when using the telephone in the secure mode so that the conversation will not be overheard by persons without the need-to-know.
   (e) Adhere to the security classification displayed on the terminal for each call.
   (f) When the terminal is keyed, limit access to those with a proper clearance and need-to-know.
   (g) Ensure that the authentication media is not left unattended in the secure phone, and that the user card is secured as a controlled cryptographic item upon completion of the call, unless located in a space approved by ADM/DFS, and certified by ADM/DFS, for open storage.

(h) Check the secure phone at the end of the day to ensure that authentication media has not been left in the unit, unless locked in a space approved by ADM/DFS, and certified by ADM/DFS, for open storage.

(i) Immediately report COMSEC incidents, as described in the National Security Agency/Central Security Service Policy Manual No. 3-16, to a COMSEC manager, or NRC COR. (Certain COMSEC incidents also may be reportable to ADM/DFS/FSB, as security incidents; refer to MD 12.1 for further guidance.)

(j) Unplug unclassified telephones from the network when the secure telephone is in use.

(k) Remove cell phone batteries or cell phones from the room when the secure telephone is in use.

K. Network Services

Network services provided in-house by NRC, other Government agencies, or by vendors must comply with NRC policies and directives and the relevant authoritative laws, Executive Orders, directives, policies, standards, or regulations. System owners shall ensure that all network services comply with CSO-STD-2003, "Network Services Standard," available from the CISO Cybersecurity Standards Web site at http://www.internal.nrc.gov/CSO/standards.html.

L. Electronic Media and Device Handling

All electronic media must be protected from unauthorized disclosure, modification, removal, and destruction. Electronic media can be either active (can manipulate information) or passive (simply provides a container). System owners shall ensure system media is either destroyed or cleaned of all information using NRC-approved data wiping techniques before the media leaves NRC control. System owners shall ensure electronic media use complies with CSO-STD-2004, "Electronic Media and Device Handling Standard," available from the OCIO Cybersecurity Standards Web site at http://www.internal.nrc.gov/CSO/standards.html.

M. Exchange of Electronic Information

Exchange of electronic information requirements are designed to protect NRC data as it flows internally within the NRC and to external parties. These requirements govern all forms of electronic communication including phone, fax, e-mail, and network communications. NRC users must protect information according to the information sensitivity level, regardless of the method of exchange.

1. Information Exchange Policies and Procedures

(a) NRC network users shall be aware of the content of the information they are communicating, who they are communicating the information with, how they are communicating the information, and where they are communicating the information, both physically and electronically.

(b) Exchanges of information and software between the NRC and other organizations should follow a formal exchange policy carried out in accordance with formal exchange agreements that comply with pertinent laws and regulations. NRC users shall follow prescribed requirements to protect the sensitivity of information exchanged with others, whether they are individuals associated with the NRC or external parties.

(c) Electronic transmissions include electronic mail, instant messaging, cloud storage, and voice calls, file transfer solutions (e.g., dropbox), as well as other electronic methods of information transfer. Electronic transmissions shall not be automatically forwarded to non-NRC electronic destinations.

(d) If a contractor employee has an NRC e-mail account, only NRC e-mails accounts shall be used to conduct business with the NRC.

(e) If a contractor employee does not have an NRC e-mail account but has an e-mail account with the contractor, only the contractor e-mail account shall be used to conduct business with the NRC.

(f) If an NRC e-mail account and a contractor e-mail account are not available, e-mail accounts personally owned by a contractor may only be used for information that is not CUI.

(g) An NRC account or system shall not be used in a manner that may give the false impression that an individual's otherwise personal communication is authorized by the NRC. If a personal e-mail or other electronic message could be misunderstood to be an official communication, a disclaimer must be used in the message. A disclaimer might appear as follows: "The following message is personal and does not reflect any official or unofficial position of the United States Nuclear Regulatory Commission."

(h) Only NRC accounts and systems shall be used to conduct official business on behalf of the agency. An e-mail or system account that an individual owns (i.e., not purchased by or maintained by NRC) shall not be used by NRC staff to conduct official NRC business.

(i) Transmission of confidentiality sensitive electronic information onto networks that are not controlled by NRC (e.g., the Internet) must be encrypted, including but not limited to electronic mail.

(j) System owners shall ensure the nature of communications exchanges are formally documented in written exchange agreements to reduce the risk that attackers may compromise the information. System owners shall ensure that sensitive unclassified information is encrypted using FIPS PUB 140-2, "Security Requirements for Cryptographic Modules," validated cryptographic modules operated in FIPS mode in accordance with OCIO-CS-STD-2009, "Cryptographic Control Standard" (formerly CSO-STD-2009). NRC information is exchanged electronically through networks including NRC's Intranet, NRC's e-mail system, and the Internet. The following

guidelines apply to all NRC users when exchanging information electronically. NRC users shall be responsible for the following:

(i) Ensure electronic information is sent to appropriate parties only.

(ii) Ensure the rules of behavior are followed for personnel, contractors, and business partners authorized to use the system and for the locations at which the system may be used.

(iii) Verify the recipient list and the individual's authorization to access the information before sending electronic transmissions.

(iv) Protect information stored electronically on NRC systems from authorized access using system controls (e.g., shared drives that can be accessed by only specific individuals or groups).

(v) Encrypt all CUI and classified information sent through untrusted networks (e.g., Internet), including but not limited to e-mail sent to non-NRC e-mail addresses.

(vi) Ensure information is provided only over networks and systems approved for the level of information.

(vii) Comply with remote access requirements.

(viii) Ensure that only individuals or computer processes acting on behalf of individuals with legitimate access authorization and a need to know have the ability to decrypt CUI and classified information.

(k) System owners shall ensure that connections to other systems are monitored, controlled, and documented. System owners are responsible for the following system connections:

(i) Ensure that communication is controlled at the external boundary of the system and at key internal boundaries within the system.

(ii) Ensure that NRC systems connect to external networks and information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the NRC enterprise architecture framework.

(iii) Ensure that the interface characteristics, security requirements, and the nature of the information communicated is documented for each interface between these systems and NRC-owned or operated information systems.

2. Additional requirements for exchanging electronic information are available on the OCIO cybersecurity Web site at http://www.internal.nrc.gov/CSO/.

N. Electronic Commerce Services

1. Electronic commerce services applications, including cloud storage services, shall use encryption to protect sensitive data at rest and in motion and shall provide

protections commensurate with the level of the risk associated with the value of the transaction and the application.

2. NRC IT system and network users shall only use NRC owned or operated IT systems that have been authorized by appropriate officials to provide electronic commerce services.

3. System owners shall ensure the integrity of NRC information that is publicly available. System owners shall ensure NRC content on publicly accessible systems is monitored for non-public information.

4. Specific security requirements on securing electronic commerce services are available on the OCIO cybersecurity Web site at http://www.internal.nrc.gov/CSO/.

O. Monitoring

1. The purpose of monitoring IT systems is to detect suspicious or unauthorized activity in computer IT systems and their underlying platforms. Monitoring requires maintaining sufficient system audit log information to allow NRC to conduct forensic reviews in the event of a system or network breach. Monitoring is used to check the status and health of NRC assets, to affirm the effectiveness of the security controls in place, to verify conformity of identification and authentication policies, and support security inquiries and investigations. System owners shall ensure monitoring addresses all federally mandated requirements, NRC-defined security requirements, and organizationally defined values.

2. All electronic systems must include display of a warning banner that provides security and legal notices to users accessing NRC information systems and requires user action to acknowledge the notices. Approved warning banners are provided in OCIO-CS-STD-0040, "Warning Banner Standard." Any updates to OCIO-CS-STD-0040 must be approved by the CIO, the Insider Threat Program's Senior Agency Official, and OGC in accordance with Executive Order 13587 and other relevant laws and regulations.

VII. ACCESS CONTROL

A. Overview

Access controls determine how users, resources, and systems interact with data and each other. Access control systems and security features are usually considered the first line of protection. These systems and features dictate how subjects access objects and resources, and the main goal is to protect the objects and resources from unauthorized access.

B. Logical Access Control

Logical access controls are computer-based access controls that provide a technical means of controlling what information users, devices, and other systems can use, the programs they can run, and the modifications they can make to NRC information and IT systems. Controlling access applies to human users as well as devices and systems.

1. All electronic CUI and classified information shall be encrypted in accordance with OCIO-CS-STD-2009 during transit and at rest.

2. To receive an ATO, an unclassified IT system must be Personal Identity Verification (PIV) enabled. An IT system is said to be PIV enabled when authorized users are able to access the system using a PIV card.
3. Logical access controls protect—
   (a) Operating systems and system software from unauthorized modification or manipulation (and thereby help ensure the system's integrity and availability);
   (b) The confidentiality, integrity, and availability of information by restricting the number of users and processes with access; and
   (c) CUI and classified information from being disclosed to unauthorized individuals.

C. A Layered Approach to Security

1. Access control requires a layered approach to security (defense-in-depth) where each possible vulnerability or attack vector (method) is identified and appropriate countermeasures are employed.
2. Access controls include the following:
   (a) Limiting network user access to drives, folders, and files;
   (b) User role restrictions;
   (c) Network perimeter access restrictions;
   (d) Controlling internal network communication devices;
   (e) Implementing filters and monitoring techniques on internal networks,
   (f) Implementing application security, and
   (g) Implementing inbound and outbound data flow controls.
3. At the NRC, access is determined on a need-to-know basis.
4. System owners shall ensure network compliance with CSO-STD-2007, “Network Access Control Standard,” available from the OCIO Cybersecurity Standards Web site at http://www.internal.nrc.gov/CSO/standards.html.

VIII. IT SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE

A. Overview

1. Cybersecurity is a critical aspect to consider during all phases of an IT system’s life cycle, including but not limited to acquisition, development, maintenance, and disposal. Adequate consideration of cybersecurity during the early stages of an IT system’s life cycle helps to ensure the IT system and the information it processes are properly protected and potential costs are identified early.

2. To ensure that necessary cybersecurity requirements have been considered, OCIO/ISPO involvement is required in all phases of an IT system's life cycle, especially before development. All IT systems, regardless of the information that they process, store, or transmit must be authorized to operate by the AO before being used in a production capacity.
3. Cybersecurity investments are made for both enterprisewide and system-level efforts. Enterprisewide investments are made for efforts that benefit all or most agency systems and improve NRC's overall security posture (e.g., boundary protection, identity management). System-specific investments are made for system-level security concerns (e.g., security control assessment, vulnerability mitigation).

B. Enterprise Architecture (EA)

Security considerations must be included as an integral component of the NRC EA.

1. Security Architecture (SA)

   (a) Contains key NRC requirements, processes, and common service attributes of the current SA, the future/target SA, and the transition plan.

   (b) Ensures identification of appropriate cybersecurity products, controls, services, and solutions to meet NRC's business security needs while minimizing the operation and maintenance burden to the agency and is documented as the NRC Enterprise Security Segment Architecture.

   (c) Applies security considerations to NRC resources, IT investments, and system development activities in a uniform and cost-effective way.

   (d) Implements identity management consistent with Section 504 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–4 274; 15 U.S.C. 7464), including multi-factor authentication, for remote access and each user account with elevated privileges.

   (e) Isolates sensitive or critical information resources (e.g., information systems, system components, applications, databases, and information) into separate security domains with appropriate levels of protection based on the sensitivity or criticality of those resources.

   (f) Implements policies of least privilege at multiple layers—network, system, application, and data—so that users have role-based access to only the information and resources that are necessary for a legitimate purpose.

   (g) Implements a policy of least functionality by only permitting the use of networks, systems, applications, and data, as well as programs, functions, ports, protocols, or services that are necessary in meeting mission or business needs.

2. System Owner

   (a) Acquires and incorporates into their systems components that are part of the NRC current or target architecture.

   (b) Incorporates shared security services as common controls as the services are implemented (e.g., the reduced sign-on infrastructure).

C. Capital Planning: Roles and Responsibilities for IT Acquisition

1. CIO

   The CIO shall review and approve all IT acquisitions and will ensure that cybersecurity is adequately addressed.

2. System Owners

   (a) Ensure a capital asset budget planning process that is consistent with OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," is followed and includes cybersecurity explicitly in IT investments and capital planning.

   (b) In coordination with the CIO and CISO, ensure that all IT resources are identified during the capital planning process.

   (c) Ensure the resources required to adequately protect the system are determined, documented, and allocated as part of the capital planning and investment control process.

   (d) Ensure the funding required to implement and maintain applicable IT cybersecurity requirements throughout the system life cycle is included in all capital investments.

   (e) Ensure specific funds for the development, modernization, or enhancement efforts required to correct cybersecurity deficiencies identified for the system are included in system funding requests and are allocated. Correction of cybersecurity deficiencies categorized as critical or high shall take precedence over other system modifications.

3. Information Technology Executive Governance

   The Information Technology Executive Governance co-chaired by the NRC CIO and CFO shall be established to direct NRC IT investment decisions and ensure appropriate consideration of cybersecurity in those investments. This organization will perform the following:

   (a) Establish cybersecurity priorities and prioritization criteria, ensuring NRC mission and vision alignment consistent with IT security priorities and criteria.

   (b) Evaluate existing and proposed IT investments against NRC's cybersecurity priorities, using prioritization criteria as a factor in determining which NRC investments to fund.

(c) Ensure the resources required to adequately protect NRC IT systems are documented and allocated as part of the capital planning and investment control process.

(d) Establish appropriate NRC IT boards to perform IT analyses and make recommendations to executive governance personnel.

(e) Assign detailed IT investment review and security analyses, including IT investment recommendations, to appropriate NRC IT boards.

4. Information Technology Boards

Established information technology boards shall conduct detailed IT investment review and security analyses (including business case reviews) and make IT investment recommendations to the Information Technology Executive Governance Organization. This analysis includes the appropriate consideration of NRC cybersecurity priorities and prioritization criteria.

D. Security in the System Development Life Cycle (SDLC): Risk Management Framework (RMF)

1. NRC Risk Management Strategy

(a) NRC uses RMF to identify, categorize (i.e., low, moderate, high), mitigate, accept, and manage IT system risk throughout the agency. Through the RMF, the agency defines acceptable risk assessment methodologies and risk mitigation strategies. The NRC SDLC shall be consistent with NIST SP 800-64, "Security Considerations in the System Development Life Cycle," NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach" (available from the NIST SP Web site at http://csrc.nist.gov/publications/PubsSPs.html), and CNSS Instruction (CNSSI) 1253, "Security Categorization and Control Selection for National Security Systems," available on the CNSS Instructions Web site at https://www.cnss.gov/CNSS/issuances/Instructions.cfm. The security assessment and authorization process integrated with the SDLC shall define the agency's processes for consistently evaluating risk across the agency with respect to the agency's risk tolerance, as well as approaches for the continuous monitoring of risk over time. The use of an IT risk executive function shall facilitate consistent, agencywide application of the risk management strategy.

(b) System owners, ISSOs, project officers, project managers, contracting officers, and others must follow the NRC SDLC for all system development and comply with MD 12.5.

(c) The RMF process transformed authorization activities to a six-step risk management framework that emphasizes building security capabilities into Federal systems through management practices and applying controls, maintaining awareness of security state, and providing information to leadership to facilitate decisions regarding acceptance of risk. Tasks

associated with the security assessment and authorization of IT systems are an integral part of the RMF. The SDLC and the security assessment and authorization processes are the means for implementing the RMF within NRC.

2. Security Authorization Tasks

   (a) The security authorization tasks directly support the determination of risk to agency operations and assets, individuals, other organizations, and the Nation that may result from the operation and use of IT systems, and ultimately, deciding if these risks are acceptable. The IT system security authorization process requires a well-defined RMF and a comprehensive set of approved IT security standards and guidelines.

   (b) The following activities describe the security authorization process:

      (i) Initiation – System boundaries along with system inputs and outputs are defined, information to be processed by the system is identified and categorized, and security requirements are documented.

      (ii) Development/acquisition – System architecture and design are completed and the system is built and tested, ensuring cybersecurity controls are appropriately implemented.

      (iii) Implementation/assessment – The system is deployed, ensuring cybersecurity controls are in place, operating as intended, and having the desired effect.

      (iv) Operations/maintenance – Continuous monitoring of security controls is performed along with vulnerability mitigation, and modifications are assessed to ensure the system security posture is not negatively impacted.

      (v) Disposal – The system is no longer operational and all components and information are disposed of securely.

   (c) Other Considerations

      (i) It is important to note that while these phases and steps may appear to be sequential, many activities are cyclical. Findings and recommendations from the security controls assessments may trigger remediation, which in turn may require reassessment of selected security controls. The level of effort and resources expended for security authorization activities should be commensurate with the security category of the system.

      (ii) The development of the system risk assessment occurs in phases. A preliminary system risk assessment must be completed before the implementation of other controls in order to complete the first two steps in the RMF. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements.

E. Correct Processing in Application

Correct processing protects information from unauthorized modification and deletion, and prevents information misuse and errors in all aspects of information processing. Applications should be designed to correctly process information, including information validation at critical points within the application (e.g., data input and output).

F. Cryptography Controls

1. Use of Cryptography at NRC

   (a) Cryptography can be used to protect the confidentiality and integrity of information. However, encrypted information is not considered to be non-sensitive. Cryptography protects information for a limited period of time. Increases in computing power have resulted in the ability to break encryption previously thought to be effective for a much longer period of time. As a result, if encrypted information is available to malicious actors, that information will be accessible by those actors over time.

   (b) Cryptography (e.g., encryption) is performed using cryptographic modules. Those cryptographic modules must be validated by an appropriate Federal authority for the level of information being processed.

2. Cryptographic Requirements

   (a) All cryptography must use FIPS 140-2 validated cryptographic modules operated in FIPS mode. Cryptographic modules used for CUI must be FIPS 140-2 validated to at least an overall level 2. Cryptographic modules used for CUI/SP-SGI must be FIPS 140-2 validated to at least an overall level 2 with the validation subcategories of Roles, Services, and Authentication; electromagnetic interference/electromagnetic compatibility; and Design Assurance validated to at least level 3.

   (b) Cryptographic modules used for classified information must be encrypted using encryption modules approved by the National Security Agency (NSA) and operated as directed by NSA for protecting classified information.

   (c) Cryptographic modules used for SCI information must be encrypted using encryption modules approved by the DNI and operated as directed by the DNI for protecting SCI information.

   (d) Additional information on cryptographic actions, uses, key strengths, and key management can be found in OCIO-CS-STD-2009, “Cryptographic Control Standard,” available from the OCIO Cybersecurity Standards Web site at http://www.internal.nrc.gov/CSO/standards.html. System owners shall ensure all use of cryptography complies with OCIO-CS-STD-2009.

   (e) The CISO should be consulted when determining cryptographic specifications. The Office of the General Counsel (OGC) should be consulted when cryptographic constructs, including electronic or digital signatures, are to be used for legal purposes or internationally.

G. Security of System Files

1. General

   The confidentiality, integrity, and availability of system files must be protected. System files may contain audit log information, or they may contain information about the business of the organization. These files may contain information that, if released to malicious users, could result in an adverse impact to the NRC, individuals, or the public. In other cases, the confidentiality is not an issue, but the loss of integrity or availability could result in an adverse impact.

2. Control of Operational Software

   (a) Operational software is executable software that is either interpretable code or executable code. Interpretable code is computer code where the source language is translated into machine language one line at a time and then executed, all within the operational environment. Executable code is computer code that has been compiled into binary machine code.

   (b) System owners shall ensure that formal procedures for system software installation, including identification of roles and responsibilities, are documented. System owners shall ensure the procedures are reviewed and updated as necessary on at least an annual basis.

   (c) Operational systems shall not contain compilers, unless specifically approved by the AO.

   (d) All code on operational systems shall be executable or interpretable code.

   (e) System owners shall ensure a current baseline configuration of the system that includes communications- and connectivity-related aspects of the system, system components, network topology, and the logical placement of the component within the system architecture, is formally documented and placed under configuration control. Additional information related to system configuration control is described in Section VI.D, “Security-Focused Configuration Management and Change Control,” of this handbook.

   (f) System owners shall ensure the following:

      (i) Software installed on the system is properly licensed for the intended use.

      (ii) Unauthorized software programs are not installed on the system.

      (iii) Modifications to the system explicitly include a security impact analysis.

      (iv) Changes to the system are analyzed by cybersecurity personnel as part of the change approval process to determine potential security impacts.

3. Protection of System Test Data

   (a) CUI and classified information shall not be stored, processed, or transmitted within the development or test environments.

(b) Test data shall not include CUI and classified information.

(c) Only test data may be used in systems that have not received an authority to operate.

4. Access Control to Program Source Code

   Access to NRC program source libraries shall be restricted so that individuals only have the required level of access to the specific library entries needed to perform legitimate business functions. System owners shall ensure source code is protected at the sensitivity level of information to be processed by the code.

H. Security in Development and Support Processes

Classified system owners shall ensure a security concept of operations (CONOPS) is developed for the IT system that contains, at a minimum, the following:

1. The purpose of the system,
2. A description of the system architecture,
3. The security authorization schedule, and
4. The security categorization and associated factors considered in determining the categorization.

I. Technical Vulnerability Management

1. OCIO/ISPO shall monitor cybersecurity vulnerabilities identified by both Federal and private sources and shall notify system ISSOs of vulnerabilities that may impact their systems.
2. OCIO/ISPO shall lead efforts to identify and mitigate vulnerabilities and deficiencies that are found in NRC IT systems. To support the identification of these vulnerabilities, system owners and ISSOs shall scan their NRC IT systems in accordance with federally mandated requirements, NRC-defined security requirements, continuous monitoring requirements, organizationally defined values, and whenever new vulnerabilities potentially affecting the system are identified. OCIO/ISPO shall work with the system owners and ISSOs to ensure a proper mitigation strategy is developed and executed for each finding. System owners and ISSOs will update vulnerability scanning mechanisms whenever new vulnerabilities are identified or reported.
3. Critical updates are fixes for security defects in operating systems and applications as well as current anti-virus definitions and other intrusion detection and prevention information. System owners shall ensure critical updates for all software are applied to systems in accordance with required configuration standards.
4. The need to apply critical updates more frequently shall be evaluated by the system ISSO at least monthly. This evaluation will take into account the nature of the critical updates issued by the operating system and software vendors, the risk to the system, and the ISSO operational experience with and knowledge of the system.

IX. CYBERSECURITY INCIDENT MANAGEMENT

A. Overview

1. A “cybersecurity threat” as defined in the Cybersecurity Act of 2015 is any action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term “cybersecurity threat” does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

2. The goal of cybersecurity incident management is to ensure incident resolution affords the maximum system and information protection and incident recovery possible. Timely notification and mitigation is essential in achieving this goal.

3. Cybersecurity Information Sharing and Analysis Centers (ISACs) are organizations where specific business sectors share cyber threat and mitigation information to assist the organizations in providing appropriate defenses. As ISACs and procedures are developed for a cybersecurity purpose, as defined in the Cybersecurity Act of 2015, and consistent with the protection of classified information, NRC may participate by sharing with or receiving from any other entity or the Federal Government a cyber-threat indicator, as defined in the Cybersecurity Act of 2015, or defensive measure.

4. FISMA requires that Federal agencies establish a cybersecurity incident response capability and designate a primary and secondary point of contact with the US-CERT. The NRC is responsible for reporting all incidents and internally documenting corrective actions and their impact. OMB requires reporting on any unauthorized release of PII, either in electronic or physical form, in which that information may be accessed by those without a need-to-know the information. NIST SP 800-61, “Computer Security Incident Handling Guide,” provides guidelines for Federal agencies on how to implement a cybersecurity incident handling capability and is available from the NIST Web site at http://csrc.nist.gov/publications/PubsSPs.html.

5. OCIO/ITSDOD shall develop formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response requirements. NRC IT system owners shall ensure host and network based intrusion detection tools are employed for moderate unclassified, high unclassified, and classified systems. As part of the NRC monitoring program, described in Section VI.O, “Monitoring,” of this handbook, the intrusion detection tools shall be configured to detect and automatically alert appropriate personnel of vulnerabilities, changes to the network, known and unknown attack signatures, and traffic anomalies.

6. NRC shall employ automated mechanisms to support the incident handling process, to increase the availability of incident response-related information, and for support.

7. Cybersecurity incidents will be handled at the appropriate level of classification, but will allow for redacted (unclassified) notification to the appropriate NRC incident management group. All incident-related information containing CUI/SP-SGI or classified information that is necessary for incident remediation will be handled on a system authorized and at the level appropriate to the information contained therein. All users and incident response persons are required to discuss, document, or otherwise process incident information in accordance with the appropriate security classification guide and NRC MDs.

B. User Reporting of Cybersecurity Incidents

1. Users

   (a) Must report any actual or potential incidents within 1 hour of discovery to the CSIRT by one of the following methods:

      (i) Select the “report a security incident” button on the upper right-hand corner of the NRC internal Web site.

      (ii) Telephone on 301-415-6666.

      (iii) Send e-mail to CS_IRT@nrc.gov.

   (b) Must report lost, damaged, or stolen computing resources (e.g., desktop computer, cell phone, BlackBerry, laptop, thumb drive) either actual or suspected, immediately to the CSIRT and to the immediate supervisor.

2. System Owners

   (a) Shall ensure malicious or suspicious events discovered by users, ISSOs, and system administrators are reported to the NRC in accordance with federally mandated requirements, NRC-defined security requirements, and organizationally defined values.

   (b) Shall ensure cybersecurity directives are implemented in accordance with OCIO/ISPO direction.

C. Report Cybersecurity Weaknesses

1. Users

   (a) Must report potential security weaknesses in IT systems or services to the CSIRT in accordance with federally mandated requirements, NRC-defined security requirements, and organizationally defined values.

   (b) Shall not attempt to correct potential weaknesses or test to determine if the weakness exists.

2. System Owners

   (a) Ensure identified weaknesses are recorded in a system POA&M.

(b) Shall not attempt to correct potential weaknesses or test to determine if the weakness exists.

D. Report Information Spills

1. An information spill is a type of incident where electronic information is placed on a system that is not approved to process that level of information. Information spills shall be reported as cybersecurity incidents to the CSIRT. The CSIRT shall report the spill immediately to ADM/DFS, OIG, the system owner, information owner, and the system ISSO.

2. The details of an information spill are as sensitive as the information that was spilled. Consequently, reporting the details of a CUI/SP-SGI or classified information spill using NRC e-mail or a standard telephone is considered a security violation. Details of CUI/SP-SGI and classified information spills must be reported in a secure manner in accordance with the level of information spilled. The CSIRT shall report the spill immediately to ADM/DFS, OIG, the system owner, information owner, and system ISSO.

3. CSIRT shall ensure classified system and data owners are contacted in a secure fashion, and classified system owners shall ensure an assessment is conducted to determine the potential impact of the spill on national security. The assessment shall be conducted in accordance with Executive Order 13526, “Classified National Security Information,” and Title 32 of the *Code of Federal Regulations* (CFR), National Defense Part 2001, “Classified National Security Information” (Information Security Oversight Office Directive No. 1). System owners shall ensure that data owners are contacted for an assessment of impact of the spill.

4. System owners shall ensure development and maintenance of procedures to isolate and contain information spills to minimize damage and to preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counter intelligence purposes. These procedures must be followed whenever an information spill occurs. All affected media must be classified/categorized at the same level as the spilled information until the information spill remediation process is completed.

5. Mitigation procedures, including disposition of affected media (i.e., sanitization, physical removal, or destruction), must be in accordance with the potential harm that may result from the compromise of spilled information.

6. Special techniques must be used to delete CUI/SP-SGI information from electronic storage media. These techniques may include destruction of the physical media, obliteration of the CUI/SP-SGI using a CISO-approved software product, or erasure of all information through use of a CISO-approved degaussing product and procedure. Guidance on CUI/SP-SGI removal from electronic media can be found on the OCIO/ISPO Incident Response Web site at http://www.internal.nrc.gov/CSO/incident-resp.html.

E. Cybersecurity Incident Response Plan

1. Overview

   The OCIO/ITSDOD is responsible for ensuring development of an agencywide Cybersecurity Incident Response Plan (CSIRP). The OCIO/ITSDOD shall review the plan no less than annually, update as required, and communicate changes.

2. Standards for Prioritizing Cybersecurity Incidents

   Cybersecurity incidents must be prioritized based on the criticality of the affected resources and the effect the incident has on the organization. Response expectations must be set by priority level. For example, the OCIO/ITSDOD incident response capability must respond to a high priority cybersecurity incident within 4 hours. The OCIO/ITSDOD shall identify and designate a list of near real-time alerts that indicate a high probability of intrusion and shall ensure intrusion detection systems are configured to monitor for those indications.

3. The Cybersecurity Incident Response Process shall contain the following:

   (a) Preparation – selecting tools, preventing and preparing for cybersecurity incidents, and annual training.

   (b) Detection and Analysis – cybersecurity incident categories, signs of an incident, sources of precursors and indications, incident analysis, incident documentation, incident prioritization, and incident notification.

   (c) Containment – containment strategy, evidence gathering and handling, identifying the attacker.

   (d) Eradication – deleting malicious code, disabling breached user accounts.

   (e) Recovery – restoring the system to normal operation and hardening the system to prevent similar cybersecurity incidents.

   (f) Post-incident Activity – incorporating lessons-learned, using collected incident data, evidence retention, assessing residual risk, coordinating incident handling activities with contingency planning.

   (g) Procedures – for testing incident response capabilities.

   (h) Recommendations – for improvement.

4. Federal Incident Reporting Guidelines

   (a) NRC staff must comply with Federal incident reporting notification guidelines on the US-CERT Web site available at https://www.us-cert.gov/.

   (b) Cybersecurity incidents shall be tracked by the CSIRT. Tracking information shall include type, volume, and cost of incident. Tracking information shall be used to identify recurring and high impact incidents along with mitigation strategies.

5. Testing

   System owners shall ensure development of system-specific incident response plans. Agencywide and system-specific incident response plans shall be tested at least annually.

F. Cybersecurity Incident Response Team (CSIRT)

1. Purpose

   (a) The OCIO/ITSDOD provides a centralized incident response capability that includes assembling resources as needed from appropriate parts of NRC. The CSIRT leader and alternate are dedicated staff whose primary purpose is to ensure a quick, effective, and orderly response to address cybersecurity incidents.

   (b) The CSIRT is staffed by—

      (i) OCIO;

      (iv) ADM/DFS, as needed;

      (v) NSIR Information Security representatives, as needed; and

      (vi) OIG Investigations Cyber Crimes Unit (CCU), as needed.

2. Responsibilities of the CSIRT

   (a) The CSIRT responsibilities are a higher priority for the OCIO team members than their other duties. Staff from NSIR and ADM shall be available, as necessary, in an expeditious manner to support the CSIRT efforts. The OCIO/ITSDOD shall provide specialized training at least annually to the CSIRT, including simulated events, to facilitate an effective response by personnel during crisis situations. Training shall include automated mechanisms to provide a more robust and realistic training environment, as appropriate.

   (b) The CSIRT shall develop a report summarizing all cybersecurity incidents and all PII incidents (whether the compromise was electronic or physical), transmitting this report to the OCIO/ITSDOD and CISO for approval, and shall notify US-CERT about malicious or suspicious activity. Cybersecurity incidents are reported to US-CERT based upon Federal incident reporting guidelines and standards.

   (c) All potential or confirmed incidents involving PII must be reported to the NRC senior agency official for privacy and to US-CERT within 1 hour of discovery, and all known or suspected instances of spillages of classified information must be immediately reported.

   (d) Classified cybersecurity incidents must follow the CNSS policies, including but not limited to CNSS Policy (CNSSP) 18, “National Policy on Classified Information Spillage,” available from the CNSS Web site at http://www.cnss.gov/policies.html, and CNSS Instruction (CNSSI) 1001, “National Instruction on Classified Information Spillage,” available from the CNSS Web site

at https://www.cnss.gov/CNSS/issuances/Instructions.cfm. For reports of spillage, apply the same protections, markings, and labeling as the sensitivity level of the data involved.

(e) The CISO shall notify the OIG of all cybersecurity incidents. Once notified, the OIG will determine their level of involvement. The OIG will coordinate with other law enforcement agencies as needed to ensure the incident has been properly addressed. If an action against a person or organization involves a matter under investigation by the OIG, then the OIG shall collect and retain the evidence for its investigation. The CSIRT shall retain and collect all other evidence that may need to be presented to law enforcement.

(f) The OCIO/ITSDOD shall test the incident response capability in accordance with CSO-STD-0020, "Organization Defined Values for System Security Controls," available from the OCIO Cybersecurity Standards Web site at http://www.internal.nrc.gov/CSO/standards.html, to determine its effectiveness and shall document test results. When possible, the OCIO/ITSDOD's evaluation of the organization's cybersecurity incident response capability employs automated mechanisms to assist in the reporting of security incidents and to more thoroughly test the organization's incident handling process.

X. BUSINESS CONTINUITY MANAGEMENT

A. Requirements for Business Continuity Management

Business Continuity Management (BCM) includes consideration of cybersecurity requirements for continued business operations subsequent to the occurrence of unplanned events that disrupt computerized business processes. For example, a disruption could be a server disk failure resulting in the loss of all information on the disk, a network failure resulting in an inability to communicate with NRC partners, or a building failure resulting in complete loss of an NRC facility.

1. System owners and common control providers must plan and prepare for disruptions.
2. Business line leads shall at least annually identify all IT systems and assets that are required to perform their business functions and shall identify those specifically required to continue critical business processes.
3. Business line leads shall identify the length of time each IT system and asset can be unavailable before critical business processes are impacted.

B. Identifying NRC Business Lines and Business Line Leads

1. The Executive Director for Operations (EDO) shall identify NRC business lines and a business line lead with responsibility for the business line.
2. Business line leads must identify the IT systems upon which the business line operations rely. In addition, business line leads also must identify critical business functions and the supporting systems that must be sustained in the event of an interruption. NRC business lines are typically supported by multiple systems.

3. A business line lead must consider the following factors:

   (a) Almost all business lines rely upon an internal network, the Internet, and e-mail.

   (b) Some business lines have systems dedicated to their business needs and some require isolated systems and networks.

   (c) Still others may require multiple systems that support multiple functional areas. For example, NRC financial systems specifically support the Office of the Chief Financial Officer (OCFO) business operations. Other business lines also may depend upon the OCFO business line.

C. Examples of Events (Threats)

Examples of events (threats) that may affect IT system availability that may lead to business disruptions include the following:

1. Natural (e.g., hurricane, tornado, flood, and fire),
2. Human (e.g., operator error, sabotage, implant of malicious code, and terrorist attacks), and
3. Environmental (e.g., equipment failure, software error, telecommunications network outage, and electric power failure).

XI. COMPLIANCE

A. Legal Requirements (Seeking Legal Advice)

Staff should seek legal advice from OGC, whenever necessary, and for the following issues:

1. Identification of applicable law,
2. Intellectual property rights,
3. Protection of agency records,
4. Data protection and privacy of personal information,
5. Prevention of misuse of computer processing facilities, and
6. Export restrictions and restrictions on sharing cryptographic information with foreign entities.

B. Compliance with Cybersecurity Policies and Standards, and Technical Compliance

1. Office of the Chief Information Officer

   The OCIO provides oversight to verify that all IT systems comply with agency IT security policies, guidance, standards, and procedures.

2. System Owners perform the following:

   (a) Conduct assessments of the security controls in their IT systems at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired cybersecurity outcome.

   (b) Ensure continuous monitoring of cybersecurity controls so that the controls are implemented correctly, operating as intended, and producing the desired outcome. They do this in accordance with CSO-PROS-1323, "U.S. Nuclear Regulatory Commission Agencywide Continuous Monitoring Program."

   (c) Implement CSO-STD-0020, "Organization Defined Values for System Security Controls," which contains NRC-defined values for NIST SP 800-53 security controls.

   (d) Ensure the security state of their systems adhere to NRC continuous monitoring requirements.

C. IT Systems Audit Considerations

The NRC recognizes the potential for interference in IT system operations as part of the system auditing process as well as the requirement to prevent any misuse of auditing tools.

1. Responsibilities

   (a) System owners shall ensure their systems produce audit records that contain sufficient information to, at a minimum, establish:

      (i) What type of event occurred,

      (ii) When (date and time) the event occurred,

      (iii) Where the event occurred,

      (iv) The source of the event,

      (v) The outcome (success or failure) of the event, and

      (vi) The identity of any user/subject associated with the event.

   (b) The ISSO shall review the audit logs to determine if there is evidence of a suspicious event or the system has undergone an attack. Suspicious events include but are not limited to the following:

      (i) Users who have misused the system,

      (ii) Privileges accidently given to a user who does not need them, and

      (iii) The system changed without authorization.

   (c) The ISSO ensures the following:

      (i) Everyone using the system is doing so within their defined roles.

(ii) Only users that have been given access are using the system.

(iii) Changes to the system have been properly approved.

(d) The ISSO shall monitor, log, and audit the execution of information system functions by privileged users (that ordinary users are not authorized to perform) to detect misuse and to help reduce the risk from insider threats.

(e) The CISO determines, based on current threat information and ongoing assessment of risk, specific events that must be audited within systems and identifies the required frequency of audits or the circumstances that require auditing.

2. Access to Audit Tools and Information

(a) Access to audit tools and the information generated by them must be protected to prevent misuse.

(b) Access to IT system audit tools and generated information shall be restricted to ISSOs, OCIO/ISPO personnel, and OIG CCU personnel.

(c) Auditing contractors shall be provided with access only for the duration of their auditing period.

(d) The audit tools and generated information shall be separated from development and operational systems when not in use.

(e) Audit results shall be encrypted for long-term storage and be protected at the overall sensitivity level of the target system, in accordance with the FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems.” FIPS PUB 199 is available on the NIST Web site at http://csrc.nist.gov/publications/PubsFIPS.html.

Exhibit 1 Abbreviations

ADM	Office of Administration
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization to Operate
BCM	Business Continuity Management
BCP	Business Continuity Plan
CCU	OIG Investigations Cyber Crime Unit
CD	Compact Disk
CFO	Chief Financial Officer
CFR	*Code of Federal Regulations*
C-I-A	[Data] Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CNSI	Confidential National Security Information
CNSS	Committee on National Security Systems
CNSSI	CNSS Instruction
CNSSP	CNSS Policy
COMSEC	Communications Security
CONOPS	Concept of Operations
CPIC	Capital Planning and Investment Control
CRD	Confidential Restricted Data
CSIRP	Cybersecurity Incident Response Plan

CSIRT	Cybersecurity Incident Response Team
CSS	Central Security Service
CUI	Controlled Unclassified Information
CUI/SP	Controlled Unclassified Information Specified
CUI/SP-SGI	Safeguards Information [Controlled Unclassified Information Specified, Safeguards Information]
CUI/SP non-SGI	Controlled Unclassified Information Specified, Non-Safeguards Information
DFS	ADM, Division of Facilities and Security
DNI	Director of National Intelligence
DOD	Department of Defense
DSO	Division of Security Operations
DVD	Digital Video Disk
EA	Enterprise Architecture
EDO	Executive Director for Operations
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act of 2014
HB	Handbook
HSPD-12	Homeland Security Presidential Directive 12
IEC	International Electrotechnical Commission
IG	Inspector General
ISAC	[Cybersecurity] Information Sharing and Analysis Centers
ISO	International Organization for Standardization

ISPO	Information Security Planning and Oversight
ISSE	Information System Security Engineer
ISSO	Information System Security Officer
IT	Information Technology
JAB	Joint Authorization Board
MD	Management Directive
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSIR	Office of Nuclear Security and Incident Response
OCFO	Office of the Chief Financial Officer
OCHCO	Office of the Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OISSO	Office ISSO
OMB	Office of Management and Budget
P2P	Peer-to-Peer
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SA	Security Architecture
SCA	Security Control Assessor
SCI	Sensitive Compartmented Information

SDLC	System Development Life Cycle
SNSI	Secret National Security Information
SODR	System Owner Designated Representative
SP	NIST Special Publication
SRD	Secret Restricted Data
US-CERT	United States Computer Emergency Readiness Team
UUI	Uncontrolled Unclassified Information