Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

Cybersecurity Act of 2015 Audit for NRC

OIG-16-A-18
August 8, 2016

All publicly available OIG reports (including this report) are accessible through NRC's Web site at http://www.nrc.gov/reading-rm/doc-collections/insp-gen

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

August 8, 2016

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: CYBERSECURITY ACT OF 2015 AUDIT FOR NRC (OIG-16-A-18)

Attached is the Office of the Inspector General's (OIG) audit report titled *Cybersecurity Act of 2015 Audit for NRC*.

The report presents the results of the subject audit. Following the August 4, 2016, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-16-A-18

August 8, 2016

Results in Brief

Why We Did This Review

The Cybersecurity Act was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States.

Division N, Section 406, of the Act requires that Inspectors General report on the policies, procedures and controls to access "covered systems." Covered systems are defined as a national security system, or a Federal computer system that provides access to personally identifiable information (PII).

The U.S. Nuclear Regulatory Commission (NRC) uses three different types of national security systems to process and store classified information: standalone systems, subscriber systems, and shared service systems. Federal policy requires that classified information may only be stored, processed, or transmitted using systems that have been granted an NRC authorization to operate for classified information processing.

The audit objective was to assess NRC's information technology (IT) security policies, procedures, practices, and capabilities relative to covered systems for national security systems and systems that provide access to PII operated by or on behalf of NRC.

Cybersecurity Act of 2015 Audit for NRC

What We Found

NRC's cybersecurity program has established policies and procedures to control access to its "covered systems." However, opportunities exist to strengthen the cybersecurity and physical security controls of NRC's national security systems.

OIG found that NRC has national security systems that were operating without the required authorizations to operate. Seven national security systems were identified, across multiple offices, as not having an authorization to operate. This occurred because there is a lack of clarity in the agencywide policies and procedures over the systems and no integrated process across relevant offices. In addition, there is no agencywide inventory of the national security systems. As a result, classified information may be vulnerable or subject to unauthorized disclosure.

In addition, OIG reviewed the policies, procedures, and controls in place for NRC systems that provide access to PII. OIG reviewed the privacy impact assessments for a sample of NRC databases that maintain PII and the system security plans for the corresponding information systems where the databases are located. Section IV of this report discuss the policies, procedures, and controls.

What We Recommend

This report makes two recommendations to improve security over NRC's national security systems information systems, ensure compliance with Federal policies through development of agencywide policies and procedures over classified information systems, and maintain an agencywide inventory of national security systems. Management stated their agreement with the finding and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS i

I. BACKGROUND 1
II. OBJECTIVE 4
III. FINDING 4
NRC Has National Security Systems Without Required Authorization to Operate 4
Recommendations 8
IV. POLICIES, PROCEDURES, AND CONTROLS PER THE CYBERSECURITY ACT OF 2015 9
V. AGENCY COMMENTS 16

APPENDIX

A. OBJECTIVE, SCOPE, AND METHODOLOGY 17

TO REPORT FRAUD, WASTE, OR ABUSE 19

COMMENTS AND SUGGESTIONS 19

ABBREVIATIONS AND ACRONYMS

CNSS	Committee on National Security Systems
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Office
IT	Information Technology
NIST	National Institute for Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

I. BACKGROUND

The Cybersecurity Act of 2015

The Cybersecurity Act of 2015 (Act) was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States. The Act aims to promote and facilitate the sharing of information across entities, both Federal and non-Federal, whose cybersecurity efforts could potentially benefit from greater access to cybersecurity-related information. In addition, the Act aims to bolster the security of the Federal government's own cyber resources.

Division N - Systems Inspectors General Must Report On

The Act at Division N, Section 406, requires Inspectors General to report to the appropriate committees of jurisdiction in the Senate and the House of Representatives on the policies, procedures, and controls to access "covered systems." The list of specific requirements is set forth in Section IV of this report.

Covered systems are defined by the Act as a national security system, or a Federal computer system that provides access to personally identifiable information (PII). This report only addresses national security systems and systems that provide access to PII. The Act does not require the Inspector General to address any other NRC information system, such as the Safeguards Information Local Area Network and Electronic Safe (SLES). [1]

A national security system is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, which involves intelligence and cryptologic activities, control of military forces, and weapons.

[1] NRC developed the Safeguards Information Local Area Network and Electronic Safe (SLES) system to store and manage electronic Safeguards Information documents. Safeguards Information is a special category of sensitive unclassified information to be protected as authorized by Section 147 of the Atomic Energy Act. It concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material.

Figure 1. Examples of PII

Source: Publicly Available Photo

PII is defined as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

What is Classified Information?

Classification is a means of identifying information concerning the national defense and foreign relations of the United States that requires protection against disclosure to unauthorized people. Classification restricts access to only properly cleared and authorized people who require access to the information to perform official duties.

NRC staff work primarily with two types of classified information:

A. National Security Information: Information classified by an Executive Order whose compromise would cause some degree of damage to the national security.
B. Restricted Data: All data concerning (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Atomic Energy Act, as amended.

National Security Systems NRC Uses

NRC personnel use three different types or categories of national security systems to process and store classified information:

A. Standalone System. A standalone laptop or desk computer not connected to a network.

B. Subscriber System. For this type of system, the sponsoring agency manages the logical access controls. An example of this type of system is the Homeland Secure Data Network (HSDN).

C. Shared Service System. For this type of system, the sponsoring agency has part of the controls, but NRC owns the directory services and maintains the terminals used to access the system.

NRC does not have a classified network of its own – it relies upon the networks of other Federal agencies. However, it has standalone computers that process and store classified information. All NRC personnel with access to any system or network (to include a stand-alone system or network) on which classified information resides, must be an NRC authorized classifier.[2]

[2] An authorized classifier is an individual authorized, in writing by appropriate authority, to classify, declassify, or downgrade classified information.

II. OBJECTIVE

The audit objective was to assess NRC's information technology (IT) security policies, procedures, practices, and capabilities relative to covered systems for national security systems and systems that provide access to personally identifiable information (PII) operated by or on behalf of NRC.

III. FINDING

NRC Has National Security Systems Without Required Authorization to Operate

NRC has national security systems that were operating without the required authorizations to operate, contrary to Federal and internal requirements. This happened because agencywide policies and procedures governing national security systems were not clear or well understood. Without agencywide policies and procedures, classified information may be vulnerable or subject to unauthorized disclosure.

What Is Required

For national security systems, NRC must adhere to Management Directive 12.5 and the Committee on National Security Standards Systems (CNSS) requirements. An authorization to operate is required for all national security systems.

NRC Management Directive 12.5. Management Directive 12.5 is NRC's internal guidance for its Cybersecurity Program. The directive lays out NRC's policy to protect information and IT systems from unauthorized access, use, disclosure, disruption, modification or

destruction. For national security systems, the management directive points to the standards and guidelines issued by CNSS. NRC must comply with CNSS policy and guidance for IT security processes, procedures, and testing. In addition, classified information must only be stored, processed, or transmitted using systems that have been granted an NRC authority to operate for classified information processing.

CNSS Policy No. 22 "Policy on Information Assurance Risk Management for National Security Systems." This policy provides the guidance and responsibilities for establishing an integrated organization-wide information assurance risk management program to achieve and maintain an acceptable level of information assurance risk for organizations that own, operate, or maintain national security systems. Appendix B, "Implementation Guidance" states that agencies must follow the National Institute for Standards and Technology (NIST) standards. NIST standards require that an authorizing official review relevant information and issue an authorization to operate for a system. All systems must have an authorization to operate issued by an NRC Designated Approving Authority in order to be able to process sensitive information.

Also, CNSS Policy No. 1253 "Security Categorization and Control Selection for National Security Systems" has additional requirements for national security systems that are not required for unclassified systems. This requires a greater effort to obtain and maintain an authorization to operate for the national security systems, than that of an unclassified system.

What We Found

NRC has national security systems that were operating without an authorization to operate or without an authorization to use. For national security systems owned by other agencies, the owning agency issues an authorization to operate and NRC must issue an authority to use.

Seven national security systems were identified, across multiple offices, as not having an authorization to operate. Additionally, four national security systems did not have an authority to use. Lastly, two laptops were identified as being used without an authorization to operate. The laptops are no longer being used and will be taken out of service.

Why This Occurred

NRC has national security systems operating without an authority to operate because there is a lack of clarity in the agencywide policies and procedures over the systems and no integrated process across relevant offices.

Multiple offices are involved in the use of national security systems. The Office of the Chief Information Officer (OCIO) is responsible for planning, directing, and overseeing the implementation of NRC's IT security program including cybersecurity. The Office of Nuclear Security and Incident Response plans, develops, establishes, and administers policies, standards, and procedures for the NRC classified information security program, and manages the security classification program. In addition there are offices that use, process, and store classified information, including the Office of Nuclear Materials Safety and Safeguards, the Office of Nuclear Regulatory Research, and the regional offices. However, there is no integrated agencywide process over the national security systems applicable to all of these offices.

More specifically, many NRC staff looked to Management Directive 12.2, "NRC's Classified Information Security Program", for direction on matters involving national security systems. Management Directive 12.2 does not specify that national security systems require an authorization to operate in accordance with Management Directive 12.5.

In addition, there is no agencywide inventory of the national security systems. The systems identified as operating without the proper authorization, were identified by the OCIO during this audit in an informal inventory conducted in April/May 2016. OCIO then decided to

conduct a formal inventory by: (1) using an Executive Director for Operations system, and (2) having the Chief Information Officer contact the offices that do not report to the Executive Director for Operations.[3] The inventory of national security systems will need to be updated periodically.

Why This Is Important

Without clear and effective agencywide policies and procedures for national security systems, classified information may be vulnerable or subject to unauthorized disclosure.

Potential system vulnerabilities. An authorization to operate is granted according to a risk-based framework that analyzes the level of risk to the information in the system. If a system is not characterized correctly, it may not have the appropriate level of protection. For example, if a hard drive with classified information is put into a computer only authorized for unclassified information, there could be an information spill and the information may be vulnerable because the computer does not have the proper protections in place.

Figure 2. A hard drive being removed from a laptop.

Source: Publicly Available Photo

Unauthorized access to classified information. Without the appropriate level of protection, there is also a potential risk of unauthorized access to classified information. OIG, however, did not

[3] The Executive Director for Operations is the chief operating office of the Commission, and is authorized and directed to discharge the operational and administrative functions necessary to the day-to-day operations of the agency.

during this audit identify any instances of unauthorized access to classified information.

No integrated approach to decommissioning systems. In addition, there is no integrated approach within NRC to take a system out of service once the system is no longer needed. However, it is imperative that NRC assign responsibility for this function so that previously operating systems can be taken out of service and disposed of properly. Moreover, without an integrated approach, the agency may be wasting resources.

Recommendations

OIG recommends that the Executive Director for Operations

1. Clarify agencywide policies and procedures over national security information systems and assign responsibility for implementing these policies and procedures.

2. Complete a comprehensive inventory of all national security information systems and review it at appropriate intervals.

IV. POLICIES, PROCEDURES, AND CONTROLS PER THE CYBERSECURITY ACT OF 2015

A. Statutory Basis for Reporting. Division N of the Cybersecurity Act of 2015, Section 406, requires Inspectors General to report on covered systems.[4]

OIG is required to report on:

1. A description of the logical access policies and practices used by NRC to access covered systems, including whether appropriate standards were followed.

2. A description and list of the logical access controls and multi-factor authentication used by NRC to govern access to covered systems by privileged users.

3. A description of information security management practices used by NRC.

4. A description of the policies and procedures of NRC with respect to ensuring that entities, including contractors, that provide services to NRC are implementing information security management practices used by NRC.

B. NRC Policies and Procedures in Place for Employees and Contractors

Management Directive 12.5 provides the management framework for the NRC Cybersecurity Program. Management Directive 12.5 contains information and references to relevant Computer Security Office (CSO)[5] issued standards for logical access controls, incident response and monitoring. The "U.S. NRC Agency-wide Rules of Behavior for Authorized Computer Use," referred to hereafter as the Rules of Behavior, is an NRC policy that specifies the user level rules for the secure use of all computing resources used to process or store sensitive NRC information. The Rules of Behavior provide quick guidelines for logical access control, authentication, protection of PII, incident reporting, and

[4] Division N of the Cybersecurity Information Sharing Act, Cybersecurity Act of 2015, Section 406, can be accessed at https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf (pages 108-113).

[5] The Computer Security Office is now the Information Security Directorate, in OCIO.

electronic data protection. Other OCIO issued standards are further detailed for the Cybersecurity Plan implementation. Additionally, Management Directive 12.2, "NRC Classified Information Security Program" provides the management framework for the classified information security program. Its objective is to ensure that all NRC personnel responsible for controlling, handling, and marking classified information and activities involving this information, adhere to the proper procedures.

Logical Access Policies and Procedures

Management Directive 12.5 states that logical access controls protect:

1. Operating systems and system software from unauthorized modification or manipulation;
2. The confidentiality, integrity, and availability of information by restricting the number of users and processes with access; and
3. Sensitive information from being disclosed to authorized individuals.

In order to gain access to any system that processes sensitive information, whether at the primary workplace, an alternative workplace, or on official travel, each authenticated user must follow and acknowledge the agencywide Rules of Behavior. All NRC employees, contractors, and other users that authenticate to NRC systems must acknowledge that they understand the user responsibilities when using NRC information technology resources. Authenticated users are to only access and use information systems for which they have official authorization.

Logical Access Controls and Multi-factor Authentication

NRC created authentication policies to ensure that only authorized persons have access to NRC information and computer systems. These policies are applicable to all NRC employees, contractors, and other users that authenticate to NRC systems and who process, store, or produce classified national security information. Authentication is strengthened by the number of incorporated authentication factors. The factors are something the user knows (password), something the user has (badge), and something the user is (biometric data). A strong password is required to protect NRC sensitive information and information systems. OCIO issued a standard with varying requirements for passwords used to protect Sensitive Unclassified Non-Safeguards Information and systems, Safeguards Information and systems, and Classified Information and systems. Following Federal requirements, NRC's information technology systems are

personal identity verification enabled to allow access using a personal identity verification card.

Information Security Practices

NRC's Computer Security Incident Response Team (CSIRT) implements the formal incident response capability. CSIRT develops and maintains all NRC cyber incident response policies, processes, incident report types and maintains applicable records, and reports incident information to the United States Computer Emergency Readiness Team, NRC management, NRC OIG, and/or other government agencies when necessary. The Rules of Behavior require all authenticated users to report suspicious activity to CSIRT.

Continuous monitoring helps maintain ongoing awareness of information security, vulnerabilities, and threats in support of NRC risk management decisions for systems storing or processing NRC information up to, and including, the Safeguards Information level. Information system continuous monitoring occurs at the agency level, business processes level, and information systems level. System owners are to ensure security controls are in place, operate as intended, and have the desired effect for both NRC established systems and other agency systems operated on behalf of NRC. Periodic reviews of the systems provide senior officials with an NRC-wide view of the agency's cybersecurity posture.

OCIO is responsible for maintaining a current and authoritative information technology system inventory. To maintain the system inventory, all hardware and software components within the system's authorization boundary, including subsystems, must be provided. Information required for the systems include the name, vendor name, version, and database.

All electronic media must be protected from unauthorized disclosure, modification, removal, and destruction. Electronic media includes hard drives, Universal Serial Bus memory sticks, Compact Disks, and magnetic tapes. Electronic media is required to be managed, labeled, and [if] encrypted at the level of information the media is used to process, transmit, or store.

Figure 3. Universal Serial Bus Memory Stick

Source: Publicly Available Photo

C. Policies and Procedures for Access to Classified Systems

Management Directive 12.5 states that classified systems are to comply with policies issued by CNSS. Specific classified information system policies are cited in Management Directive 12.5, as well as in OCIO guidance.

- CNSS Policy No. 22, "Policy on Information Assurance Risk Management for National Security Systems," provides the guidance and responsibilities for establishing an integrated, organization-wide information assurance risk management program to achieve and maintain an acceptable level of information assurance risk for organizations that own, operate, or maintain national security systems.
- CNSS Policy No. 18, "National Policy on Classified Information Spillage," requires agencies that own or operate information systems used to collect, generate, process, store, display, or transmit/receive national security information to establish policies and procedures for handling classified information spillage. NRC has training that includes the process to handle classified information spills, including alerting CSIRT.
- CNSS Instruction No. 1001, "National Instruction on Classified Information Spillage," establishes the minimum actions required when responding to an information spillage of classified national security information onto a classified information system.
- CNSS Policy No. 26, "National Policy on Reducing the Risk of Removable Media," establishes the criteria for the use of removable media in national security systems, and includes information on mitigation techniques.

D. NRC's Systems that Provide Access to PII

NRC's Privacy Act Systems of Records

In 2015, NRC conducted a comprehensive review of all its Privacy Act systems of records notices.[6] The systems of records notice lists 38 systems maintained by NRC that contain personal information about individuals from which information is retrieved by an individual's name or identifier. The systems of records are databases whose records are located inside of a system.

The audit team conducted a sample of the databases and interviewed the system managers of those selected for information on logical access policy and controls. The nine databases selected in the sample were:

1. Contracts Records
2. Employee Assistance Program Records
3. Employee Locator Records
4. Freedom of Information Act and Privacy Act Request Records
5. Occupational Injury and Illness Records
6. Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records
7. Oral History Program
8. Personnel Security Files and Associated Records
9. Strategic Workforce Planning Records

Interviews with the system managers revealed that these databases contained PII such as name, social security number, date of birth, medical information, and employment information for NRC employees and contractors. This information is either maintained in hardcopy or electronic format. If electronic, it may be on the personal drive of a system manager, a Universal Serial Bus drive, stored in the system server, or the system may be owned by a contractor or another Federal agency where information will be accessed online. Access to most of the databases are restricted to registered/approved individuals, or are role-based. Access is granted through the personal identity verification card or NRC Local Access Network ID, soft certifications, or by login-password. If there is contractor access, NRC policies are to be followed. If there is an information spill, CSIRT is notified, or agency policies are followed for reporting.

[6] The 2015 NRC Privacy Act Systems of Records Notices can be accessed at http://www.nrc.gov/reading-rm/foia/privacy-act-records.pdf.

Federal Information Security Modernization Act of 2015 (FISMA) Report

As of the completion of fieldwork for the fiscal year 2015 FISMA report, NRC has 23 operational information systems. The systems that corresponded with the database sample are:

1. ACCESS (Automated Access Control and Computer Enhanced Security System)
2. ADAMS (Agencywide Documents Access and Management System)
3. FAIMIS (Financial Accounting & Integrated Management Information System)
4. ITI (Information Technology Infrastructure)
5. MASS (Moderate ADM Support Systems)
6. STAQS (Strategic Acquisition System)

E. System Security Plans and Privacy Impact Assessments

Privacy Impact Assessments

The audit team reviewed Privacy Impact Assessments[7] (PIA) for the databases selected in the sample. The databases with a PIA in place collectively contained PII about Federal NRC employees, Federal contractors, NRC licensees, consultants, foreign assignees, and the public. Individuals that have access to the information stored in these databases are specific NRC employees that have role-based access. The Strategic Workforce Planning Records are also accessible to all NRC employees to access their own information, and the Freedom of Information Act and Privacy Act Request Records have limited access to external agencies, organizations, and the public. Users are able to gain access to these databases with two-factor authentication, and/or a user profile that has been assigned with a password.

Some systems did not have a PIA in place because they were not electronic databases, did not hold information for more than nine individuals, or were in the process of obtaining one.

[7] A Privacy Impact Assessment is an analysis of how information is handled to ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy. The process helps identify systems that handle information in identifiable form about individuals to ensure that appropriate information assurance measures are in place.

System Security Plans

NIST Special Publication 800-53, Revision 4, "Standards and Privacy Controls for Federal Information Systems and Organizations" provides a catalog of security and privacy controls for Federal information systems. The controls are meant to protect organizational operations, organizational assets, individuals, other organizations, and the nation from hostile cyber attacks, natural disasters, structural failures, and human errors. NRC has a system security plan template for these customizable controls.

The security controls reviewed for the selected FISMA reported systems were Access Control, Identification and Authentication, Incident Response, Media Protection, and System and Information Integrity. Logical access policies and controls were found in management directives, OCIO policies, or information system specific procedures. All systems use least-privilege access.[8] Four of the systems follow agency issued identification and authentication guidance. One system's policies are contained in its own guidance. One system did not have the security control in place for identification and authentication policy, but it is planned. Passwords or personal identity verification cards are used to access agency workstations for five of the systems. If a password is used, the system either follows agency issued password policy, or adheres to a system specific password policy.

Non-organizational users do not have access to any of the six systems. All of the systems had incident response policy and procedures in place, citing CSIRT, specific information system procedures, or that the services were contracted. There were also policies in place for continuous monitoring. Media protection policy and procedures were agency-issued, relied on another system for protection, or the information system's specific policy are used.

Although not part of the requirements, the privacy controls were reviewed. Most systems did not contain PII, so controls were not applicable, or were left out of the system security plan completely. The systems that do contain PII have a PIA in place; however, one system reviewed did not fully comply with three of the privacy controls. The Chief Information Officer is aware of this and is working to gather further information on the issue.

[8] The principle of least-privilege access allows only authorized access for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

V. AGENCY COMMENTS

A discussion draft of this report was provided to NRC prior to an exit conference held on August 4, 2016. NRC management provided comments that have been incorporated into this report, as appropriate. As a result, NRC management stated their general agreement with the report and will not provide formal comments.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to assess NRC's information technology (IT) security policies, procedures, practices, and capabilities relative to covered systems for national security systems and systems that provide access to personally identifiable information (PII) operated by or on behalf of NRC.

Scope

The audit focused on the policies, procedures, and controls used to access national security systems and those systems that provide access to PII.

OIG conducted this performance audit at NRC headquarters in Rockville, Maryland from March 2016 to June 2016. OIG also reviewed and analyzed internal controls related to the audit objective. Throughout the audit, auditors were aware of the possibility of fraud, waste, and abuse in the program.

Methodology

OIG reviewed relevant Federal laws and standards including

- The Cybersecurity Information Sharing Act of 2015.
- The Privacy Act of 1974.
- CNSS Policy 22, “Policy on Information Assurance Risk Management for National Security Systems.”
- NIST 800-53, “Guidance for Security and Privacy Controls for Federal Information Systems and Organizations on Identification and Authentication of Organizational Users.”

To understand the policies and procedures in place for logical access controls on NRC's national security systems, OIG reviewed additional internal documents, including:

- Management Directive and Handbook 12.2, "NRC Classified Information Security Program."
- Management Directive and Handbook 12.4, "NRC Communications Security (COMSEC) Program."
- Management Directive and Handbook 12.5, "NRC's Cybersecurity Program."

In addition, OIG identified NRC's 38 systems of records reported in the Federal Register per the Privacy Act of 1974. OIG selected a sample of 9 systems of record for review, and reviewed the PIAs for each of these databases. OIG then identified which NRC systems these databases are located on and reviewed the system security plan for each system.

OIG interviewed NRC staff and management to gather information on logical access controls for national security systems and systems that have access to PII. Auditors interviewed personnel from the OCIO, Office of Nuclear Security and Incident Response, the Office of the Chief Human Capital Officer, the Office of Administration, and the Office of the Chief Financial Officer.

We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by Beth Serepca, Team Leader; Kristen Lipuma, Audit Manager; Ziad Buhaissi, Senior Auditor; Ebaide Esoimeme, Auditor; Janelle Wiggs, Auditor; and Chanel Stridiron, Auditor.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TDD 1-800-270-2787

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.