OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017

OIG-18-A-02
October 30, 2017

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

October 30, 2017

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017 (OIG-18-A-02)

Attached is the Office of the Inspector General's (OIG) independent evaluation report titled *Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014* [FISMA 2014] *for Fiscal Year 2017*. The purpose of this evaluation was to perform an independent evaluation of NRC's implementation of FISMA 2014 for Fiscal Year 2017.

The report presents the results of the subject evaluation. Following the October 17, 2017, exit conference, agency management indicated that they had no formal comments for inclusion in this report.

NRC has made significant improvements in the effectiveness of their information technology (IT) security program, and continues to make improvements in performing continuous monitoring activities. However, the evaluation identified the following IT security program areas that need improvement: (1) IT security program documentation is not up-to-date; and (2) some continuous monitoring activities were not performed as required.

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 evaluation. 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-18-A-02
October 30, 2017

Results in Brief

Why We Did This Review

The Federal Information Security Modernization Act of 2014 (FISMA 2014) outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor. The Office of Management and Budget (OMB) requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

The evaluation objective was to perform an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA 2014 for Fiscal Year 2017.

Independent Evaluation of NRC's Implementation of FISMA 2014 for Fiscal Year 2017

What We Found

NRC has made significant improvements in the effectiveness of their information technology security program, and continues to make improvements in performing continuous monitoring activities. However, the independent evaluation identified the following information technology security program areas that need improvement:

- Information technology security program documentation, including policies, processes, procedures, guidance, standards, and templates are not up-to-date.
- Some continuous monitoring activities were not performed as required. Specifically, some security categorizations, contingency plans, and business impact assessments are not updated annually as required.

What We Recommend

To improve NRC's implementation of FISMA, we make seven recommendations. Management stated their general agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

AO	Authorizing Official
ATO	Authorization to Operate
ATO-CA	Continuous ATO
BIA	Business Impact Assessment
DAA	Designated Approving Authority
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IT	Information Technology
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication

I. BACKGROUND

On December 18, 2014, the President signed the Federal Information Security Modernization Act of 2014 (FISMA 2014), reforming the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[1] and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor. Office of Management and Budget (OMB) memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 16, 2017, requires OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

The U.S. Nuclear Regulatory Commission (NRC) OIG retained Richard S. Carson & Associates, Inc., to perform an independent evaluation of NRC's implementation of FISMA 2014 for fiscal year (FY) 2017. This report presents the results of that independent evaluation.

[1] NRC uses the term "information security program" to describe its program for ensuring that various types of sensitive information are handled appropriately and are protected from unauthorized disclosure in accordance with pertinent laws, Executive orders, management directives, and applicable directives of other Federal agencies and organizations. For the purposes of FISMA, the agency uses the term "information technology security program."

II. OBJECTIVE

The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017.

III. ACCOMPLISHMENTS

NRC has made significant improvements in the effectiveness of their information technology (IT) security program, and continues to make improvements in performing continuous monitoring activities, as noted in Appendix B. The following are some highlights of NRC's accomplishments during FY 2017:

- An ongoing project to reduce the time needed to patch internal workstations and servers has resulted in a 50 percent reduction in vulnerabilities over the past 12 months.

- NRC completed security assessment and authorization of the NRC general support system, including 7 of the 10 subsystems, comprising over 5,000 individual components.

- NRC remediated all remaining findings from prior FISMA evaluations with the exception of three of the five findings from the FY 2016 evaluation. Two of those findings are scheduled for completion by the end of December 2017.

- NRC made significant progress in performing oversight of contractor systems (a finding from the FY 2016 FISMA evaluation).[2] As of the completion of fieldwork, 23 of the 27 contractor services/systems have a short-term authorization to operate.[3] NRC developed a comprehensive inventory of contractor

[2] Contractor systems include systems and services that are provided (in full or in part) by another Federal agency, outsourced to a commercial vendor, and cloud solutions such as software-as-a-service.

[3] Per the agency's authorization plan, short-term authorizations are granted while documentation is collected/developed (as needed), assessments are performed, and information on risks is presented to the NRC Authorizing Official to make a decision on whether a full authorization is warranted for each service.

services/systems and developed an authorization plan with three phases for completing appropriate authorization activities for them. Phase 1 began on August 7, 2017, and the authorization packages for the services/systems included in this phase will be submitted by January 31, 2018.

- NRC updated the *NRC Information Security Program Plan*, which provides an overview of the security requirements for the NRC-wide information security program and describes the program management and common controls in place or planned for meeting those requirements. NRC also performed a periodic assessment of all 185 security, program, and privacy controls that are common or hybrid with a common component.

NRC also made significant progress in performing oversight of national security systems. NRC developed a comprehensive inventory of national security systems and is making progress on completing appropriate authorization activities for them.

IV. FINDINGS

Some IT Security Program Areas Need Improvement

While NRC has made significant improvements in the effectiveness of their IT security program, the independent evaluation identified the following IT security program areas that need improvement:

- IT security program documentation, including policies, processes, procedures, guidance, standards, and templates are not up-to-date.

- Some continuous monitoring activities were not performed as required. Specifically, some security categorizations, contingency plans, and business impact assessments (BIA) are not updated annually as required.

A. IT Security Program Documentation Is Not Up-To-Date

NRC standards and instructions specify the frequency of reviewing and updating IT security program documentation. However, the majority of NRC's IT security program documentation is not up-to-date. These documents have not been updated because responsibilities for IT security program documentation maintenance have changed, guidance is not current, and documentation maintenance is not a priority. Up-to-date documentation is important for NRC staff to effectively implement the NRC IT security program.

What Is Required

Internal Requirements for Policies and Procedures

NRC standard ISD-STD-0020, *Organization Defined Values for System Security Controls*, defines the mandatory values for specific controls in the security control families described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The standard requires that documented policies and procedures to facilitate the implementation of a control should be reviewed and updated annually.

NRC office instruction CSO-ADM-0200, *Preparing and Maintaining NRC Cyber Security Processes, Procedures, Guidance, Templates, and Checklists*, requires a formal review at least annually to ensure the guidance remains accurate and effective.

What We Found

NRC IT Security Program Documents Are Not Reviewed and Updated Annually As Required

The majority of NRC's IT security program documentation is not up-to-date, including policies, processes, procedures, guidance, standards, and

templates. Many of these documents have not been updated in more than 2 years. The following are some examples:

- Risk Management Framework and Authorization Process, August 25, 2011.
- Authority to Use Process, February 15, 2014.
- IT System Decommissioning and Disposal Process, December 15, 2013.
- System Cybersecurity Assessment Process, August 1, 2015.
- Information Security Continuous Monitoring Process, April 15, 2015.
- Organization-Defined Values for System Security and Privacy Controls, August 1, 2015.
- Common and Hybrid Security Control Standard, September 1, 2015.
- Enterprise Risk Management Program Plan, October 25, 2013.

Three of the four documents that form the basis of NRC's enterprise architecture have not been updated in over 3 years.

- Network Protocol Standard, December 1, 2010.
- Remote Access Security Standard, June 1, 2015.
- Endpoint Protection Security Standard, July 20, 2014.
- Network Infrastructure Standard, including Network Interconnection Diagrams, July 18, 2014.

The configuration standards for laptops are so out dated (dated in 2009 or 2011) that they are no longer practical.

Why This Occurred

Responsibilities for IT Security Program Documentation Maintenance Have Changed

In January 2017, the Office of the Chief Information Officer (OCIO) underwent a significant reorganization. Prior to that change, there were multiple organizations within OCIO with some responsibility for maintaining IT security program documentation.

IT Security Program Documentation Maintenance Guidance Is Not Current

NRC office instruction CSO-ADM-0200, *Preparing and Maintaining NRC Cyber Security Processes, Procedures, Guidance, Templates, and Checklists*, has not been updated since April 2013. The evaluation team could not determine if this office instruction is even in use as it no longer appears on the new OCIO Procedures and Guidance Web page on the NRC intranet.

IT Security Program Documentation Maintenance Is Not a Priority

NRC stated that maintaining IT security program documentation was not a priority in the past, due to limited resources and other more urgent priorities such as performing continuous monitoring activities.

Why This Is Important

More Up-to-Date Documentation Would Lead to a More Consistently Implemented IT Security Program

Up-to-date documentation is important for NRC staff to effectively implement the NRC IT security program. It is also important for ensuring that the NRC IT security program aligns with agency and higher-level Federal Government policies, as well as applicable Federal regulations and laws. Further, up-to-date documentation helps ensure consistent IT

security practices in the face of staff turnover or changes in IT security positions.

Recommendations

OIG recommends that the Executive Director for Operations

1. Perform a gap analysis to identify required IT security program documents, IT security program documents that need to be developed, and IT security program documents that need to be updated and/or finalized.

2. Develop a schedule for developing, updating, and completing all required IT security program documentation.

3. Develop policies and procedures for keeping IT security program documentation up-to-date.

B. Some Continuous Monitoring Activities Were Not Performed As Required

FISMA 2014, NIST, and NRC define processes for performing continuous monitoring of systems owned and used by NRC in order to ensure office directors, regional administrators, and system owners are effectively managing cyber risk. In addition, NRC uses a Cybersecurity Risk Dashboard (Dashboard) to actively monitor and report on continuous monitoring activities as part of their risk management program. While NRC has made improvements in performing periodic system cybersecurity assessments, other continuous monitoring activities were not performed as required. Specifically, some security categorizations, contingency plans, and BIAs were not updated annually as required. These activities were not performed because security categorization procedures are being updated, the status of security categorizations, and contingency plan and BIA updates, is not visible in the Dashboard, and there are no procedures for monitoring completion of all continuous monitoring activities, including those that are not explicitly tracked on the Dashboard. As a result, NRC is not compliant with its own continuous monitoring program.

What Is Required

Federal Guidance Regarding Continuous Monitoring

FISMA 2014 requires that agencies establish a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and emphasizes the importance of continuously monitoring information system security. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Step 6 of the risk management framework, ongoing or continuous monitoring, is a critical part of that risk management process and allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

Internal Guidance Regarding Continuous Monitoring

NRC Continuous Monitoring Program

NRC process ISD-PROS-1323 defines NRC's process for performing continuous monitoring of systems owned and used by NRC, and involves five key tasks, including maintaining system security documentation, as well as the frequencies for which continuous monitoring activities must be performed. In addition, each year, the Executive Director for Operations issues a memorandum requiring system owners to perform cybersecurity risk management activities required for FISMA. Systems operating under a continuous[4] authorization to operate (ATO-CA) must follow the instructions in the annual risk management activities memorandum. Security categorizations, contingency plans, and BIAs must be reviewed and updated at least annually.

[4] NIST uses the term "ongoing authorization."

NRC Cybersecurity Risk Dashboard

NRC uses a Dashboard to actively monitor and report on continuous monitoring activities as part of their risk management program. The Dashboard provides a high-level view of the agency's security risk by depicting the current risk posture and the status of security risk management activities. One section of the Dashboard provides a visual representation of the status of continuous monitoring activities, including the ability to drill down to a more detailed continuous monitoring status report and a continuous monitoring metric for each system.

What We Found

Security Categorizations Are Not Reviewed and Updated Annually

NRC updated only seven security categorizations in FY 2017. Figure 1 summarizes the status of security categorizations that were not updated in FY 2017. Of the 15 that were not updated, 6 security categorizations are more than 3 years old.

Figure 1: Security Categorization Status

ATO Type	# Not Updated in FY 2017	Security Categorization
ATO	1	High: 1
ATO-CA	11	High: 2 Moderate: 9
ATO Extension	3	High: 1 Moderate: 2

Source: OIG-generated from analysis of agency documentation

Contingency Plans and BIAs Are Not Reviewed and Updated Annually

NRC did not update six contingency plans in FY 2017. Figure 2 summarizes the status of contingency plans that were not updated in FY 2017. One system's contingency plan has not been updated since May 2013; however the system's security plan indicates the contingency plan is

updated annually. The contingency plan is missing an interconnection with another operational system in a diagram, the points of contact list is not up-to-date, the software versions are incorrect, and the location of some of the servers is incorrect.

Figure 2: Contingency Plan Status

ATO Type	# Not Updated in FY 2017	Security Categorization
ATO-CA	4	Moderate: 4
ATO Extension	2	Moderate: 2

Source: OIG-generated from analysis of agency documentation

NRC did not update six BIAs in FY 2017. Figure 3 summarizes the status of BIAs that were not updated in FY 2017. Furthermore, NRC did not provide any BIAs for four operational systems.

Figure 3: BIA Status

ATO Type	# Not Updated in FY 2017	Security Categorization
ATO-CA	4	Moderate: 4
ATO Extension	2	High: 1 Moderate: 1

Source: OIG-generated from analysis of agency documentation

Why This Occurred

Security Categorization Procedures Are Being Updated

NRC is working on a new process for performing security categorizations, so system owners were instructed to delay their updates until the new process was in place. The new process will include a follow-up with system owners on their continuous monitoring activities. NRC is also considering using the Dashboard to automate some of this process.

Status of Security Categorizations, Contingency Plan Updates, and BIAs Is Not Visible in the Dashboard

The continuous monitoring activities section of the Cybersecurity Risk Dashboard does not visually present the status of security categorization or BIA updates. The Dashboard does show the status of contingency plan testing, but does not show the status of contingency plan updates. The supporting continuous monitoring status report captures security categorization status, but not BIA status. The report implies that contingency plan updates are included with the contingency plan testing; however, some of the systems with a Green (completed) status for that activity do not have updated contingency plans. In addition, the continuous monitoring metric does not factor in status of security categorizations, BIAs, or contingency plan updates.

Procedures for Monitoring Completion of All Continuous Monitoring Activities Are Lacking

In April 20, 2015, NRC decided to stop tracking low risk weaknesses on system POA&Ms. The security plans for two systems indicate that their contingency plans are outdated. However, since these weaknesses are not being tracked on the systems' POA&Ms, the system owners may overlook the need to update their contingency plans since the status of contingency plan updates is not explicitly tracked in the Dashboard.

Why This Is Important

NRC Is Not Compliant With Its Own Continuous Monitoring Program

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. For systems operating under an ATO-CA, continuous monitoring is essential for determining risk associated with systems and for ensuring risk-based decisions are made concerning continued system operation.

Recommendations

OIG recommends that the Executive Director for Operations

4. Develop and implement a schedule for reviewing and updating all security categorizations.

5. Develop and implement a schedule for reviewing and updating all business impact assessments and for developing them if they are missing.

6. Develop and implement a schedule for reviewing and updating all contingency plans.

7. Develop procedures for monitoring completion of all continuous monitoring activities, including those that are not explicitly tracked on the Cybersecurity Risk Dashboard.

V. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Perform a gap analysis to identify required IT security program documents, IT security program documents that need to be developed, and IT security program documents that need to be updated and/or finalized.

2. Develop a schedule for developing, updating, and completing all required IT security program documentation.

3. Develop policies and procedures for keeping IT security program documentation up-to-date.

4. Develop and implement a schedule for reviewing and updating all security categorizations.

5. Develop and implement a schedule for reviewing and updating all business impact assessments and for developing them if they are missing.

6. Develop and implement a schedule for reviewing and updating all contingency plans.

7. Develop procedures for monitoring completion of all continuous monitoring activities, including those that are not explicitly tracked on the Cybersecurity Risk Dashboard.

VI. AGENCY COMMENTS

An exit conference was held with the agency on October 17, 2017, at which time agency management provided comments on a discussion draft which have been incorporated, as appropriate, into this report. As a result, agency management stated their general agreement with the findings and recommendations and opted not to provide formal comments for inclusion in this report.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017.

Scope

The evaluation focused on reviewing NRC's implementation of FISMA 2014 for FY 2017. The evaluation included an assessment of the effectiveness of the NRC's information security policies, procedures, and practices, and a review of information security policies, procedures, and practices of a representative subset of NRC's information systems, including contractor systems and systems provided by other Federal agencies. Four NRC systems were selected for evaluation.

FISMA 2014 also requires agencies to ensure the adequate protection of agency information, including national security systems. The annual independent evaluation of FISMA relating to national security systems shall be performed only by an entity designated by the agency head. In FY 2016, the NRC OIG was designated as the entity responsible for performing the national security systems portion of the annual independent evaluation of NRC's information security program and practices. The evaluation team reviewed the inventory of national security systems and supporting authorization documentation for those systems.

The evaluation was conducted at NRC headquarters from June 2017 through September 2017. Any information received from NRC subsequent to the completion of fieldwork was incorporated when possible. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, evaluators considered the possibility of fraud, waste, and abuse in the program.

Methodology

Richard S. Carson & Associates, Inc., conducted an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017. In addition to an assessment of the effectiveness of the NRC's information security policies, procedures, and practices, the evaluation included an assessment of the following topics specified in OMB's FY 2017 Inspector General FISMA Reporting Metrics:

- Risk Management.
- Configuration Management.
- Identity and Access Management.
- Security Training.
- Information Security Continuous Monitoring.
- Incident Response.
- Contingency Planning.

To conduct the independent evaluation, the team reviewed the following:

- NRC policies, procedures, and guidance specific to NRC's IT security program and its implementation of FISMA 2014, and to the seven topics specified in OMB's reporting metrics.
- Security assessment and authorization documents for the four systems selected for evaluation during the FY 2017 independent evaluation, including security assessment reports and vulnerability assessment reports prepared in support of system security assessment and authorization.
- Security categorizations, security plans, contingency plans, contingency plan test reports, and ATO memoranda for NRC systems.

- Periodic system cybersecurity assessment reports for NRC systems.

When reviewing assessment reports, the team focused on security controls specific to the eight topics specified in OMB's reporting metrics.

All analyses were performed in accordance with guidance from the following:

- NIST standards and guidelines.
- Council of the Inspectors General on Integrity & Efficiency, *Quality Standards for Inspection and Evaluation*, January 2012.
- Management Directive and Handbook 12.5, *NRC Cybersecurity Program*.
- NRC Information Security Planning and Oversight Branch policies, processes, procedures, standards, and guidelines.
- NRC OIG guidance.

The evaluation work was conducted by Jane M. Laroussi, CISSP, and Maya Tyler, from Richard S. Carson & Associates, Inc.

Appendix B

CONTINUOUS MONITORING ACTIVITIES PERFORMED IN FY 2017

Improvements in Performing Continuous Monitoring Activities

NRC continues to make improvements in performing continuous monitoring activities, as illustrated by the following examples:

- NRC continued to maintain current authorizations to operate for most NRC and contractor systems. In FY 2017, NRC completed security assessments and authorizations of two systems, and for the majority of their general support system. Three additional systems were issued extensions to their ATOs. As of the completion of fieldwork for FY 2017, 19 of the 22 operational information systems[5] had an ATO. Three systems are operating under an ATO extension.[6] See Figure 4 for additional details on operational systems operating under an ATO Extension.

Figure 4: NRC Systems with an ATO Extension

System	ATO Expiration	ATO Extension Expiration	Comments
System 1	06/30/17	12/29/17	Current ATO Extension granted on 4/12/17.
System 2	02/26/16	12/31/17	Current ATO Extension granted on 1/13/17.

[5] At the end of FY 2016, the NRC had 22 operational systems. Since FY 2016, one system was decommissioned/incorporated into existing system boundaries, and one transitioned to a cloud software-as-a-service. Two new systems were added to the inventory in FY 2017, resulting in a net of 22 operational systems.

[6] Under certain circumstances, the NRC Designated Approving Authority/Authorizing Official (DAA/AO), who assumes the responsibility for operating an information system at an acceptable level of risk, can grant permission to delay the reauthorization of a system due to the need to continually operate the system in support of the agency's mission. A system owner can request the delay in writing and explain the circumstances (e.g., delays in starting testing, hardware/software upgrades, changes to the system boundary) causing the delay. The DAA/AO responds with a memorandum granting the delay and includes specific conditions that the system owner must meet to minimize the risk of operating the system under the ATO extension.

System	ATO Expiration	ATO Extension Expiration	Comments
System 3	07/26/13	07/31/18	Current ATO Extension granted on 6/13/17. This system has been operating under some type of ATO extension or short-term ATO since 2013.

Source: OIG-generated from analysis of agency documentation

- NRC updated security plans for 20 operational information systems, and 19 of the 20 are being updated quarterly as required. All 20 are compliant with NIST SP 800-53.

- NRC completed periodic system cybersecurity assessments for 18 operational information systems, and security control assessments in support of system authorization for 3 operational information systems.

- NRC updated the contingency plans for 14 operational information systems, and completed annual contingency plan testing for 14 operational information systems and for some components of 1 additional system. NRC determined that one system does not require a contingency plan or contingency plan testing.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TTY/TDD: 7-1-1, or 1-800-201-7165

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.