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 2016

OIG-17-A-03
November 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

November 8, 2016

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 2016 (OIG-17-A-03)

Attached is the Office of the Inspector General's independent evaluation report titled *Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014* [FISMA 2014] *for Fiscal Year 2016*. The purpose of this evaluation was to perform an independent evaluation of NRC's implementation of FISMA 2014 for Fiscal Year 2016.

This report presents the results of the subject evaluation. Following the November 1, 2016, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

NRC has continued to make improvements in its information technology security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations. However, the independent evaluation identified the following information technology security program weaknesses: (1) continuous monitoring is not performed as required; (2) the NRC system inventory is not up-to-date; and (3) NRC did not provide sufficient documentation to determine if oversight of contractor systems is adequate.

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-17-A-03

November 8 , 2016

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 2016.

Independent Evaluation of NRC's Implementation of FISMA 2014 for Fiscal Year 2016

What We Found

NRC has continued to make improvements in its information technology security program and progress in implementing the recommendations resulting from previous FISMA evaluations. However, we found three repeat findings from previous FISMA evaluations. Specifically, we found that continuous monitoring is not performed as required, and the NRC system inventory is not up-to-date. In addition, the agency did not provide sufficient documentation to determine if oversight of contractor systems is adequate.

What We Recommend

To improve NRC's implementation of FISMA, we made five 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
ATU	Authorization to Utilize
CCB	Configuration Control Board
CIO	Chief Information Officer
CP	Contingency Plan
DAA	Designated Approving Authority
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ISD	Information Security Directorate
IT	Information Technology
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSICD	NRC System Information Control Database
OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
PSCA	Periodic System Cybersecurity Assessment
RMF	Risk Management Framework
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.[2] Office of Management and Budget (OMB) memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2015, 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) 2016. This report presents the results of that independent evaluation. Carson & Associates will also submit responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool in accordance with OMB guidance.

[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.

[2] While FISMA uses the language "independent external auditor," OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, clarified this requirement by stating, "Within the context of FISMA, an audit is not contemplated. By requiring an evaluation but not an audit, FISMA intended to provide Inspectors General some flexibility…."

II. OBJECTIVE

The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2016. Appendix A contains a description of the evaluation objective, scope, and methodology.

III. FINDINGS

NRC has continued to make improvements to its information technology (IT) security program and progress in implementing the recommendations resulting from previous FISMA evaluations. NRC has accomplished the following since the FY 2015 FISMA independent evaluation:

- NRC continued to maintain current authorizations to operate for most NRC and contractor systems. In FY 2016, NRC completed security assessments and authorizations of three systems. Three additional systems were issued short-term authorizations to operate (ATO). As of the completion of fieldwork for FY 2016, 20 of the 22 operational information systems had an ATO. Two systems are operating under an ATO extension.[3] See Appendix B for additional information on these two systems.

- NRC updated security plans for 20 operational information systems. All 20 have been updated to be compliant with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

[3] 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.

- NRC completed periodic system cybersecurity assessments for 14 operational information systems, and security control assessments in support of system authorization for 3 operational information systems.

- NRC completed annual contingency plan testing for 13 operational information systems and for some components of 2 additional systems.

- NRC updated the contingency plans for 14 operational information systems.

- NRC established an IT Configuration Control Board (CCB) to support the efforts of the NRC Chief Information Officer (CIO) and other NRC offices in implementing consistent IT life cycle management best practices based on NRC management directives and policies as well as NIST guidelines. In addition, NRC issued three documents supporting the change management process: Information Security Directorate (ISD)[4] ISD-STD-6001, *System Change Cybersecurity Significance Standard*; OCIO-CCB-0001, *System Change Significance Determination and Notification Process*; and OCIO-CCB-0002, *Change Approval Process*.

- NRC issued a few new or updated documents and processes related to IT security including six templates.

- NRC established an Insider Threat Program Policy in accordance with Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," and the Atomic Energy Act of 1954, as amended.

While NRC has continued to make improvements in its IT security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified the following IT security program weaknesses:

[4] As of November 1, 2015, the Computer Security Office became the Information Security Directorate.

- There is a repeat finding from a previous FISMA evaluation: continuous monitoring is not performed as required.

- There is a repeat finding from previous FISMA evaluations: the NRC system inventory is not up-to-date.

- There is a repeat finding from previous FISMA evaluations: the agency did not provide sufficient documentation to determine if oversight of contractor systems is adequate.

A. Continuous Monitoring Is Not Performed as Required

Step 6 of the NIST Risk Management Framework (RMF), ongoing or continuous monitoring, is a critical part of organization-wide risk management. 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 a continuous[5] ATO (ATO-CA), continuous monitoring is essential for determining risk associated with systems and for ensuring risk-based decisions are made concerning continued system operation.

ISD process ISD-PROS-1323, *Information Security Continuous Monitoring Process*, defines the process that must be followed to perform continuous monitoring on systems owned and used by NRC. However, some of the required continuous monitoring activities have not been performed. As a result, NRC cannot ensure the effectiveness of information security controls for NRC systems and cannot identify and control risk.

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. FISMA

[5] NIST uses the term ongoing authorization.

emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct security control assessments at a frequency depending on risk, but no less than annually. FISMA also mandates that agencies follow NIST standards and guidelines to establish and secure that framework.

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 RMF, ongoing or continuous monitoring, is a critical part of that risk management process.

Key activities performed during Step 6 include the following:

- Determining the security impact of proposed or actual changes to the information system and its environment of operation.

- Assessing a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

The implementation of a continuous monitoring program results in ongoing updates to the security plan (including the risk assessment), the security assessment report, and the plan of action and milestones (POA&M).

Internal Guidance Regarding Continuous Monitoring

NRC Continuous Monitoring Program

ISD-PROS-1323 defines the process that must be followed to perform continuous monitoring on systems owned and used by the agency, and involves five key tasks, as follows:

- Assessing security control effectiveness.

- Addressing risks identified during assessments.

- Maintaining system security documentation.

- Performing required tests.

- Reporting the security state of systems to designated organization officials.

The frequencies for which continuous monitoring activities must be performed are defined in a companion document to ISD-PROS-1323. All testing activities must be completed and the final test reports dated within the required time frame (e.g., 1 year) of the previous test report date.

Each year, the Executive Director for Operations issues a memorandum requiring system owners to perform cybersecurity risk management activities required for FISMA. The purpose of these activities is to ensure office directors and regional administrators are effectively managing cyber risk. NRC uses its Cybersecurity Risk Dashboard to specify the status and current due dates of each required activity.

In the FY 2016 memorandum, issued March 2016, system owners were required to take the following actions:

- Perform a Periodic System Cybersecurity Assessment (PSCA).

- Perform an annual Contingency Plan (CP) test and complete an updated CP, CP Test Plan, and CP Test Report.

- Update all security-related documentation (e.g., System Security Plan, POA&M, Security Categorization). System security plans and POA&Ms must be reviewed at least quarterly.

The memorandum also stated that ISD and the Office of the Executive Director for Operations will ticket overdue cybersecurity requirements.

Continuous Monitoring for Systems Issued an ATO-CA

NRC is transitioning to a continuous authorization process and has implemented a policy that requires a full system authorization process be completed prior to the system entering into a continuous authorization state. The NRC Designated Approving Authority accepts the risk of operating the system in a continuing authorization state and requires use

of continuous monitoring processes to determine risks associated with the system and ensure risk-based decisions are made concerning continued system operation. Systems issued an ATO-CA must follow the instructions in the annual risk management activities memorandum, and use the security impact analysis process for system changes.

Common and Hybrid Security Control Standard

ISD-STD-0021, *Common and Hybrid Security Control Standard*, provides common and hybrid security controls required for NRC systems, identifies the common and hybrid security control providers, and defines their responsibilities for the common and hybrid security controls. The common security control providers are office directors or regional administrators with responsibility for specific types of NRC-wide security controls. They are responsible for the development, implementation, assessment, and monitoring of specific common security controls and are held accountable for the security risk associated with operating the common security controls. Common control providers are also responsible for ensuring required security documentation is prepared and maintained for each common control.

What We Found

Noncompliance With Continuous Monitoring Guidance

Required continuous monitoring activities were not performed for all NRC Systems. Figure 1 summarizes the required continuous monitoring activities that were not performed by NRC in FY 2016. For one of the systems operating under an ATO-CA, NRC has not performed any of the required continuous monitoring activities noted on Figure 1 since its ATO-CA was issued in September 2013.

Figure 1: Continuous Monitoring Activities Not Performed in FY 2016

Required Activity	# Non-Compliant Systems	Security Categorization	ATO Status
Periodic System Cybersecurity Assessment	5	High: 1 Moderate: 4	ATO: 2 ATO-CA: 3
Annual Contingency Plan Testing	7	High: 1 Moderate: 6	ATO: 2 ATO-CA: 4 ATO Extension: 1
Annual Contingency Plan Update	8 (2 not updated since 2012, repeat finding from 2014 & 2015; 2 not updated since 2013, repeat finding from 2015)	Moderate: 8	ATO: 1 ATO-CA: 6 ATO-Extension: 1
Annual Security Plan Update	2	Moderate: 2	ATO: 1 ATO-CA: 1

Source: OIG-generated figures from analysis of agency documentation

Some Periodic System Cybersecurity Assessments Were Delayed

Of the 17 systems that had a PSCA completed in FY 2016, 8 were not completed within 1 year of the previous year's testing. This is a higher percentage than in FY 2015, when 5 of 19 were delayed.

Some System Security Plans Were Not Updated Quarterly as Required

Of the 20 system security plans updated in FY 2016, 3 were not updated quarterly as required. Per the FY 2016 risk management activities memorandum, the security plans should have had an update for the fourth quarter, to be completed by August 15, 2016; however, two of the three were last updated in June 2016, and the third was last updated in April 2016.

NRC Has Not Demonstrated That Common Controls Have Been Tested

As required by ISD-STD-0021, common control providers are also responsible for ensuring required security documentation is prepared and maintained for each common control. NRC has not provided documentation demonstrating that common controls that are not provided by a specific system, such as program management controls, have been tested as part of continuous monitoring.

Why This Is Important

NRC Cannot Ensure Effectiveness of Security Controls

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. If continuous monitoring activities are not performed as required, NRC cannot ensure the effectiveness of the information security controls for NRC systems and cannot identify and control risk.

Recommendation

OIG recommends that the Executive Director for Operations

1. Develop a plan and schedule for ensuring all common controls are tested in accordance with NRC's continuous monitoring process.

B. NRC System Inventory Is Not Up-to-Date

FISMA and NIST define the requirements for developing and maintaining an inventory of information systems. ISD-PROS-2030, *NRC RMF and Authorization Process*, defines six types of systems comprising the NRC system inventory. To address findings from previous independent evaluations regarding NRC's inventory, NRC developed the NRC System

Information Control Database (NSICD), to serve as the single repository for necessary data about NRC IT investments. NRC also developed system inventory instructions that are issued with an annual system inventory data call. However, the evaluation team found that despite these instructions, NRC's system inventory is not up-to-date. As a result, NRC cannot determine whether the security controls for all NRC systems are effectively implemented and whether they are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

What Is Required

Federal Inventory Requirements

FISMA requires agencies to develop and maintain an inventory of major information systems (including major national security systems) operated by or under control of the agency. The inventory must be updated at least annually and used to support information resources management. NIST SP 800-53, control PM-5, also requires organizations to develop and maintain an inventory of its information systems.

Internal Inventory Requirements

Management Directive and Handbook 12.5, *NRC Cybersecurity Program*, and ISD-STD-0021, require the Office of Information Services (OIS) to maintain a current and authoritative IT system inventory.

ISD-PROS-2030 defines the following categories of systems. Each system in the NRC inventory should be classified as one of these system types.

- **IT System** – a compilation of hardware and software that operates within its own authorization boundary to electronically perform a specific task or set of tasks. IT Systems are NRC-owned, NRC contractor systems, or customized implementations of systems for NRC, and they exist in their own authorization boundary (i.e., not part of another system's authorization boundary).

- **Application** – computer software designed to perform singular or multiple related specific tasks. Applications are NRC commercial

off-the-shelf, Government off-the-shelf, or custom software; do not have the security infrastructure or foundation to exist in their own authorization boundary; and are part of an IT System's authorization boundary.

- **Laptops and Stand-Alone Personal Computers** – non-centrally managed laptops and stand-alone personal computers, including those processing sensitive unclassified non-safeguards information, safeguards information, and classified information (does not include laptops and desktops that are part of the NRC infrastructure system's boundary).

- **Service** – external services that support NRC's operational mission. Examples include public Web site hosting and external Government or private contractor applications/services (non-NRC).

- **Facility** – physical building leased or owned by a contractor or other Government agency to host NRC systems. IT components hosted in the facility must have an IT System ATO.

- **Social Media** – public Web 2.0 Web sites owned and operated by an external third-party (e.g., Facebook, Flickr, Twitter, and YouTube).

Each year, NRC issues a data call to all offices to review and update their system inventory information. OIS developed a SharePoint site to collect all the necessary data and developed system inventory instructions that are issued with an annual system inventory data call.

What We Found

NRC System Inventory Is Not Up-to-Date

NRC did not provide the OIG with a complete inventory for review. NRC only provided a spreadsheet containing 21 systems categorized as IT Systems in accordance with ISD-PROS-2030. NRC periodically publishes an extract from NSICD (last extract was June 2, 2016) on an internal SharePoint site. Since NRC did not provide a more current extract from NSICD to review, the evaluation team reviewed the inventory on the

SharePoint site. Since the NSICD extract on the SharePoint site contains only a subset of inventory information from NSICD, the evaluation team also reviewed inventory information collected during the most recent system inventory data call. The following are some examples of missing or incomplete information observed in the NSICD extract on the SharePoint site and inventory data call information:

- One system is incorrectly classified as an Application when it is an IT System.
- Over 40 Applications are listed without a "parent" IT System.
- Only some subsystems of one IT System are listed.
- One cloud-based contractor system is not on the inventory.

Issues with the NRC's system inventory were also identified in their FY 2016 CyberStat session and U.S. Government Accountability Office report GAO-16-511, *Agencies Need to Improve Their Application Inventories to Achieve Additional Savings*. Additionally, issues with an inventory of NRC's classified systems were identified in OIG's report OIG-16-A-16, *Cybersecurity Act of 2015 Audit for NRC*.

Why This Is Important

NRC Cannot Ensure Effectiveness of Security Controls

Without a current system inventory, NRC cannot determine whether the security controls for all NRC systems are effectively implemented and whether they are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Recommendations

OIG recommends that the Executive Director for Operations

2. Develop a plan and schedule for developing a comprehensive inventory of all NRC systems.

3. Develop supporting processes, procedures, and guidance for ensuring the NRC system inventory is maintained.

C. Insufficient Documentation Provided to Determine if Oversight of Contractor Systems Is Adequate

FISMA 2014 requires agencies to ensure the adequate protection of agency information, including information collected or maintained by contractors, as well as information systems operated by contractors on the agencies' behalf. NRC has policies for performing oversight of contractor systems. However, NRC did not provide a current system inventory of all contractor systems and did not provide requested documentation to demonstrate oversight of contractor systems is performed.

In addition, two corrective actions from the FY 2013 FISMA evaluation related to oversight of contractor systems were reported completed by NRC in September 2015; however, NRC did not provide sufficient evidence that these recommendations were actually completed. As a result, as in FY 2015, the FY 2016 evaluation team was unable to determine if oversight of contractor systems is adequate.

What Is Required

Federal Requirements for Oversight of Contractor Systems

FISMA 2014, Section 3554(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3554(b) requires each agency to provide information security for the information and "information systems that support the operations and assets of NRC, including those provided or managed by another agency, contractor, or other source." This includes 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.

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed for all contractor systems. Agencies must ensure identical, not "equivalent," security procedures. For example, annual testing and evaluation, risk

assessments, security plans, security control assessments, contingency planning, and security authorization must also be performed for all contractor systems.

Internal Requirements for Oversight of Contractor Systems

Management Directive and Handbook 12.5, *NRC Cybersecurity Program*, require Federal agencies or third-party service providers hosting NRC capabilities to meet NRC cyber security requirements. ISD-PROS-2030 describes the process for applying the RMF described in NIST SP 800-37, to secure NRC systems, including contractor systems.

ISD-PROS-2030 defines the following categories of systems and their authorization requirements. These requirements apply to NRC systems and to systems operated on the agency's behalf by contractors or other entities.

- **IT System** – requires an ATO.
- **Application** – inherits the ATO from its host IT System.
- **Laptops and Stand-Alone Personal Computers** – requires laptop certification.
- **Service** – requires an Authorization to Utilize (ATU). If the Service is not authorized to operate by another Federal agency, then it must be authorized to operate by the NRC as an IT System.
- **Facility** – requires a Facility ATO. If the Facility ATO is not issued by another Federal agency, then additional authorization requirements apply.
- **Social Media** – requires a Web 2.0 Implementation ATO.

ISD-PROS-1323 also defines the process that must be followed to perform continuous monitoring on systems owned and used by NRC, including systems owned and/or operated by other agencies. Once a Service is issued an ATU, it also requires confirmation of annual system security plan updates, annual contingency plan testing, and annual security control testing.

Each year, the NRC Executive Director for Operations issues a memorandum requiring system owners to perform cybersecurity risk management activities required for FISMA. The FY 2016 memorandum states that continuous monitoring requirements apply to NRC established systems (including contractor systems), cloud-based systems, and other external federal agency systems used by NRC. The frequencies for which continuous monitoring activities must be performed for systems with an ATU are defined in a companion document to ISD-PROS-1323 and include, but are not limited to the following:

- Ensure that the sponsoring agency maintains the system ATO in accordance with NIST SP 800-37 and provides a copy of the most recent sponsoring agency-issued ATO memorandum.

- Submit evidence of the execution of annual contingency plan testing and periodic security control testing to the ISD within one year and one month of the previous test report date.

What We Found

Insufficient Documentation Provided

As stated previously, NRC provided only a spreadsheet containing 21 systems categorized as IT Systems, of which only 2 are contractor systems. NRC did not provide a current system inventory of all contractor systems (e.g., system categorized as "Services") and did not provide requested documentation to demonstrate oversight of contractor systems is performed.

In addition, two corrective actions from the FY 2013 FISMA evaluation related to oversight of contractor systems were reported completed by NRC in September 2015. The agency stated they completed authorization of all systems categorized as contractor systems, but only provided documentation for two that are categorized as IT Systems. The agency also stated that ISD-PROS-1323 includes the explicit requirement that all contractor systems be authorized as per NRC policy and the next annual risk management activities memorandum will reference ISD-PROS-1323. While these documents describe risk management activities

for contractor systems, NRC failed to provide any evidence that such activities were actually completed. This is the second year for which NRC did not provide sufficient evidence to demonstrate oversight of contractor systems is adequate.

Why This Is Important

Adequacy of Oversight of Contractor Systems Could Not Be Determined

Without a current system inventory of all contractor systems or documentation required by the NRC continuous monitoring program for systems authorized by other agencies, the FY 2016 evaluation team was unable to determine if oversight of contractor systems is adequate.

Recommendations

OIG recommends that the Executive Director for Operations

4. Based on the updated inventory of contractor systems, identify those that are not compliant with ISD-PROS-2030, *NRC Risk Management Framework*, and complete appropriate authorization activities for those systems.

5. Develop procedures for ensuring the annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Develop a plan and schedule for ensuring all common controls are tested in accordance with NRC's continuous monitoring process.

2. Develop a plan and schedule for developing a comprehensive inventory of all NRC systems.

3. Develop supporting processes, procedures, and guidance for ensuring the NRC system inventory is maintained.

4. Based on the updated inventory of contractor systems, identify those that are not compliant with ISD-PROS-2030, *NRC Risk Management Framework*, and complete appropriate authorization activities for those systems.

5. Develop procedures for ensuring the annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

V. AGENCY COMMENTS

A discussion draft of this report was provided to the agency prior to an exit conference held on November 1, 2016. At this meeting, agency management stated their general agreement with the findings in this report 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 2016.

Scope

The evaluation focused on reviewing NRC's implementation of FISMA 2014 for FY 2016. 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. A recent OIG audit of NRC's implementation of the Cybersecurity Act of 2015[6] found that there is a lack of clarity in the agencywide policies and procedures for national security systems, no integrated process across relevant offices, and no agencywide inventory of national security systems. Therefore, for FY 2016, the evaluation team determined there was insufficient information to determine the effectiveness of the NRC's information security policies, procedures, and practices for such systems.

The evaluation was conducted at NRC headquarters from July 2016 through October 2016. Any information received from NRC subsequent to the completion of fieldwork was incorporated when possible. Internal

[6] OIG-16-A-18, Cybersecurity Act of 2015 Audit for NRC dated August 8, 2016.

controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, evaluators were aware of 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 2016. 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 2016 Inspector General FISMA Reporting Metrics:

- Risk Management, including Plan of Action and Milestones.
- Contractor Systems.
- Configuration Management.
- Identity and Access Management, including Remote Access Management.
- Security and Privacy Training.
- Information Security Continuous Monitoring.
- Incident Response Program.
- 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 eight topics specified in OMB's reporting metrics.
- Security assessment and authorization documents for the four systems selected for evaluation during the FY 2016 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 Directorate policies, processes, procedures, standards, and guidelines.

- NRC OIG guidance.

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

Appendix B

SYSTEMS WITH ATO EXTENSIONS

The following table provides additional details on operational systems operating under an ATO Extension.

Figure 2: NRC Systems With an ATO Extension

System	ATO Expiration	ATO Extension Expiration	Comments
System 1	11/16/14	09/30/17	Current ATO Extension granted on 09/28/16. This system has been operating under some type of ATO extension since 12/22/14.
System 2	09/28/14	12/23/16	Current ATO Extension granted on 03/20/16. This system has been operating under some type of ATO extension since 09/17/14.

Source: OIG-generated information from analysis of agency documentation

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.