

EVALUATION REPORT

Independent Evaluation of NRC's Implementation
of the Federal Information Security Management Act
(FISMA) for Fiscal Year 2012

OIG-13-A-03 November 8, 2012



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/>

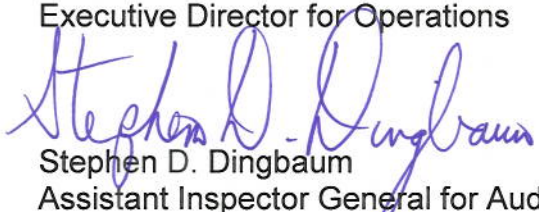


UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

November 8, 2012

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: 
Stephen D. Dingbaum
Assistant Inspector General for Audits

SUBJECT: INDEPENDENT EVALUATION OF NRC'S
IMPLEMENTATION OF THE FEDERAL INFORMATION
SECURITY MANAGEMENT ACT (FISMA) FOR FISCAL
YEAR 2012 (OIG-13-A-03)

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 Management Act (FISMA) for Fiscal Year 2012 (OIG-13-A-03)*.

The report presents the results of the subject evaluation. Agency comments provided during a November 1, 2012, exit conference have been incorporated, as appropriate, into this report.

Please provide information on actions taken or planned on 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 415-5915 or Beth Serepca, Team Leader, at 415-5911.

Attachment: As stated



**Independent Evaluation of
NRC's Implementation of the
Federal Information Security Management Act
for Fiscal Year 2012**

**Contract Number: GS-00F-0001N
Delivery Order Number: 20291**

November 7, 2012

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

The U.S. Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) retained Richard S. Carson & Associates, Inc. (Carson Associates), to perform an independent evaluation of NRC's implementation of the Federal Information Security Management Act (FISMA) for fiscal year (FY) 2012. This report presents the results of that independent evaluation. Carson Associates also submitted responses to the Office of Management and Budget's (OMB) annual FISMA reporting questions for OIGs via OMB's automated collection tool.

OBJECTIVE

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2012.

RESULTS IN BRIEF

Program Enhancements and Improvements

NRC has continued to make improvements to its information technology (IT) security program and progress in implementing the recommendations resulting from previous FISMA evaluations. The agency has accomplished the following since the FY 2011 FISMA independent evaluation:

- The agency continued to maintain current authorizations to operate for all agency and contractor systems. In FY 2012, the agency completed security assessments and authorizations of eight systems. As of the completion of fieldwork for FY 2012, all 20 operational NRC information systems and both systems used or operated by a contractor or other organization on behalf of the agency had a current authorization to operate.
- The agency completed or updated security plans for all agency and contractor systems.
- The agency completed annual security control testing for 16 agency systems and both contractor systems. Two agency systems are currently undergoing security test and evaluation in support of system reauthorization. The remaining two systems completed annual security control testing late in FY 2011 and are currently undergoing FY 2013 annual security control testing.
- The agency completed annual contingency plan testing for all agency contractor systems, and updated the contingency plans for 18 agency systems and both contractor systems.

- The agency issued several updated Computer Security Office documents, processes, and standards, including the NRC Information Security Program Plan, Continuity of Operations Plan, and several incident response documents.

Program Weaknesses

While the agency 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 information system security program weaknesses.

- The NRC system inventory is not up-to-date.
- Information system component inventories at NRC remote locations are not up-to-date.
- The NRC plan of action and milestone (POA&M) process is not consistently followed.
- The NRC POA&M tool does not consistently implement key OMB and NRC POA&M requirements.
- Contingency planning for the NRC IT environment needs improvement.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve NRC's information system security program and implementation of FISMA. A consolidated list of recommendations appears on page 15 of this report.

AGENCY COMMENTS

At an exit conference on November 1, 2012, agency officials agreed with the report's findings and recommendations. Subsequent to the exit conference, the agency provided informal comments, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

ABBREVIATIONS AND ACRONYMS

Carson Associates	Richard S. Carson and Associates, Inc.
COOP	Continuity of Operations Plan
CSO	Computer Security Office
FISMA	Federal Information Security Management Act
FY	Fiscal Year
ISCP	Information System Contingency Plan
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
SP	Special Publication

[Page intentionally left blank]

TABLE OF CONTENTS

Executive Summary	i
Abbreviations and Acronyms	iii
1 Background.....	1
2 Objective.....	1
3 Findings.....	2
3.1 FISMA Systems Inventory	2
Finding #1: NRC System Inventory Is Not Up-to-Date.....	3
3.1.1 NRC Inventory Requirements.....	3
3.1.2 Agency Procedures Are Not Followed.....	4
3.2 Configuration Management.....	5
FINDING #2: Information System Component Inventories at NRC Remote Locations Are Not Up-To-Date	5
3.2.1 Requirements for Inventory of System Components	5
3.2.2 Agency Has Not Fully Met Requirements	6
3.3 Plan of Action and Milestones (POA&M).....	7
Finding #3: NRC POA&M Process Is Not Consistently Followed	7
3.3.1 POA&M Process Requirements.....	7
3.3.2 Agency Has Not Fully Met Requirements	8
Finding #4: POA&M Tool Does Not Consistency Implement Key OMB and NRC POA&M Requirements.....	9
3.4 Contingency Planning	10
3.4.1 Background	10
3.4.2 Contingency Planning Requirements and Definitions.....	11
FINDING #5: Contingency Planning for the NRC IT Environment Needs Improvement.....	11
4 Consolidated List of Recommendations	15
5 Agency Comments	17
Appendix. OBJECTIVE, SCOPE, AND METHODOLOGY.....	19

[Page intentionally left blank]

1 Background

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002.¹ FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program² 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 compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines. FISMA requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor.³ Office of Management and Budget (OMB) memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated October 2, 2012, 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. (Carson Associates), to perform an independent evaluation of NRC's implementation of FISMA for fiscal year (FY) 2012. This report presents the results of that independent evaluation. Carson Associates also submitted responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool. A consolidated list of recommendations appears on page 15.

2 Objective

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2012. The report appendix contains a description of the evaluation objective, scope, and methodology.

¹ The Federal Information Security Management Act of 2002 was enacted on December 17, 2002, as part of the E-Government Act of 2002 (Public Law 107-347) and replaces the Government Information Security Reform Act, which expired in November 2002.

² 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 (IT) security program.

³ 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...."

3 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. The agency has accomplished the following since the FY 2011 FISMA independent evaluation:

- The agency continued to maintain current authorizations to operate for all agency and contractor systems. In FY 2012, the agency completed security assessments and authorizations of eight systems. As of the completion of fieldwork for FY 2012, all 20 operational NRC information systems and both systems used or operated by a contractor or other organization on behalf of the agency had a current authorization to operate.
- The agency completed or updated security plans for all agency and contractor systems.
- The agency completed annual security control testing for 16 agency systems and both contractor systems. Two agency systems are currently undergoing security test and evaluation in support of system reauthorization. The remaining two systems completed annual security control testing late in FY 2011 and are currently undergoing FY 2013 annual security control testing.
- The agency completed annual contingency plan testing for all agency contractor systems, and updated the contingency plans for 18 agency systems and both contractor systems.
- The agency issued several updated Computer Security Office documents, processes, and standards, including the NRC Information Security Program Plan, Continuity of Operations Plan, and several incident response documents.

While the agency 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 information system security program weaknesses.

- The NRC system inventory is not up-to-date.
- Information system component inventories at NRC remote locations are not up-to-date.
- The NRC plan of action and milestone (POA&M) process is not consistently followed.
- The NRC POA&M tool does not consistently implement key OMB and NRC POA&M requirements.
- Contingency planning for the NRC IT environment needs improvement.

3.1 FISMA Systems Inventory

FISMA and the National Institute of Standards and Technology (NIST) define the requirements for developing and maintaining an inventory of its information systems. To address findings from previous independent evaluations regarding the agency's inventory, the agency developed an automated inventory system, the NRC System Information Control Database (NSICD), to house the inventory of automated information systems. The agency also developed procedures, guides, and user manuals that provide guidance for maintaining system inventory records within

NSICD. However, the evaluation team found that despite these procedures, guides, and user manuals, the agency's system inventory is not up-to-date.

Finding #1: NRC System Inventory Is Not Up-to-Date

In response to recommendations from previous independent evaluations, the agency developed an automated inventory system and developed procedures, guides, and user manuals that provide guidance for maintaining system inventory records within that system. These procedures, guides and user manuals describe the system inventory process, the basic requirements for entering new system inventory data into NSICD, the methodology for entering data into security records within NSICD, and instructions on working with system inventory and security program information in ClearQuest. The agency also provides inventory instructions with its biannual inventory update data call. However, despite all of these instructions, the NRC system inventory is not up-to-date.

3.1.1 NRC Inventory Requirements

NRC has several procedures, guide, and user manuals that provide guidance for maintaining system inventory records within NSICD. These include:

- OIS-9000D-0002, Revision 0; *Entering New System Inventory Data in the NRC System Information Control Database (NSICD)*, June 4, 2007 – describes the basic requirements for entering new system inventory data into NSICD.
- *Administrative Guide for Entering Data Into the NSICD Security Record*, Version 1.4, June 22, 2012 – describes the methodology for entering data into security records within NSICD.
- *NSICD User Guide – Using Rational ClearQuest*, March 2, 2011 – describes the system inventory process and provides instructions on working with system inventory and security program information in ClearQuest.

The agency also provides inventory instructions with its biannual inventory update data call, as described in OIS-9000D-0001, *Biannual Automated Information System Inventory Update Procedure*, dated March 5, 2007. Twice a year (typically in January and August), the agency sends out a request to update the information contained in NSICD for automated information systems used by each NRC office.

Several organizations are responsible for maintaining system inventory records within NSICD. According to OIS-9000D-0002, the Enterprise Architecture team is responsible for adding any new system to the system inventory records in NSICD and the Computer Security Team should notify the system inventory maintainer if documentation is submitted for a system that cannot be identified within the system inventory records of NSICD. *The Administrative Guide for Entering Data Into the NSICD Security Record* states that data to be entered into the security record comes from the security documents submitted to the Computer Security Office (CSO) and from the documents created by the CSO. The *NSICD User Guide* states that system owners notify the Office of Information Services (OIS) of changes in the system inventory, in coordination with

the Office of the Chief Financial Officer, through the biannual data calls as part of the capitalization of hardware and software.

3.1.2 Agency Procedures Are Not Followed

Carson Associates is also conducting information security risk evaluations of NRC remote locations (i.e., those NRC offices located outside of the NRC headquarters complex). During site visits to three of the remote locations, the evaluation team compared the agency's inventory data from NSICD with the systems actually in place in those locations. The evaluation team found that not all systems in place at NRC remote locations are reflected in NSICD.

For example, a laptop system in one of the remote locations, which was authorized to operate December 1, 2011, is not reflected in NSICD. Authorization of this system to operate should have alerted some organization to enter this system into NSICD, but it is unclear which organization has that responsibility. For example, OIS-9000D-0002 states that new systems are initiated by submitting a screening form for a capital planning investment control review. However, laptop systems typically do not require such a review. In addition, instructions included with the biannual inventory update data call only ask system owners to update information extracted from NSICD. The instructions do not include a requirement to notify the agency of any new systems that are not reflected in the data call.

Two of the other remote locations also had some laptops used for processing safeguards information that were no longer used, but had yet to be surplus. These locations were unaware that the agency was still tracking them as active systems in the agency's official inventory as they were not included in the data provided to those locations in the biannual inventory update data call. According to the agency, they perform data calls on IT systems that are part of its portfolio of systems. The agency does not ordinarily perform a data call on independent standalone hardware, even if the hardware is used as a sensitive processor and has an NSICD system inventory numbers. The agency considers standalone hardware as assets, not systems. Therefore, NRC remote locations were not aware they needed to provide the agency with updated information regarding the status of these laptops or that they were required to follow a specific process for decommissioning these systems.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Update all procedures, guides, and user manuals that provide guidance for maintaining system inventory records within NSICD to clearly define which organization(s) are responsible for adding new system inventory records in NSICD.
2. Update the instructions included with the biannual inventory update to require system owners to notify the agency of any new systems that are not reflected in the data call.
3. Include all systems in NSICD, including all independent standalone hardware that has an NSICD system inventory number, in future biannual inventory update data calls.

3.2 Configuration Management

NIST defines requirements for developing, documenting, and maintaining an inventory of information system components as part of configuration management for a system. While information system component inventories exist for individual NRC systems, there are no up-to-date consolidated inventories for the components of these systems located in the remote locations, associated rack diagrams are not up-to-date, and the inventories that do exist do not meet NRC requirements.

FINDING #2: Information System Component Inventories at NRC Remote Locations Are Not Up-To-Date

In addition to headquarters, NRC has remote locations that conduct inspection, enforcement, investigation, licensing, and emergency response programs for nuclear reactors, fuel facilities, and materials licensees. NRC also has a remote location that provides training to meet the integrated NRC staff needs in the curriculum areas of reactor technology, probabilistic risk assessment, engineering support, radiation protection, fuel cycle, security and safeguards, and regulatory skills. These remote locations house IT system components from multiple NRC systems, including infrastructure and the badging system, as well as NRC-managed systems that support the remote location. One of the remote locations also houses IT system components supporting the NRC Continuity of Operations Plan (COOP) and IT system components that provide disaster recovery support for some NRC systems and another remote location also houses IT system components that provide disaster recovery support for some NRC systems.

During site visits to three NRC remote locations, the evaluation team found that while information system component inventories exist for individual NRC systems, there are no up-to-date consolidated inventories for the components of these systems located in the remote locations, associated rack diagrams are not up-to-date, and the inventories do not meet NRC requirements.

3.2.1 Requirements for Inventory of System Components

NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, requires organizations develop, document, and maintain an inventory of information system components. NIST SP 800-53 also requires organizations to update the inventory of information system components as an integral part of component installations, removals, and information system updates.

CSO-STD-0020, *Organization Defined Values for System Security Controls*, requires component inventories to include the following elements:

- System Name.
- Asset Name.
- Asset Type (e.g., firewall, server, workstation, etc.).
- Manufacturer.

- Manufacturer Model Number / Version.
- Manufacturer Serial Number.
- Asset Tag (if owned/leased by NRC).
- Unique Host Name (if available the host's fully qualified domain name should be used).
- Location (e.g., site, building, and room where the asset is located).
- Operating System Name.
- Operating System Version.
- Licensing Information.
- License Expiration Date.

3.2.2 Agency Has Not Fully Met Requirements

IT system components located in NRC remote locations are managed by multiple organizations and support multiple NRC systems. Even though these components are not all managed by NRC staff at that location, it is important that NRC remote locations have information on these components to easily locate and identify them in the event of a security incident or emergency.

During site visits to three NRC remote locations, the evaluation team compared inventory information and rack diagrams provided by NRC staff at these locations with the actual IT system components located in their server rooms and telecommunications closets. In each of the three remote locations, the evaluation team found that the inventory information provided did not accurately reflect all the IT system components in these locations. The evaluation team also found that the rack diagrams were not up-to-date and were missing IT system components recently added to the location. The team also found that the inventories did not include all data elements specified in CSO-STD-0020.

NIST SP 800-53 requires organizations to update the inventory of information system components as an integral part of component installations, removals, and information system updates. However, NRC has not clearly identified who is responsible for performing these activities in situations where IT system components for multiple NRC systems are located in a single location such as an NRC remote location. For example, should the agency detect unusual network activity originating from a particular network address, it would be important to have a comprehensive and up-to-date inventory of all IT system components' network addresses so the staff at the remote location can quickly identify, locate, and isolate the IT system component involved. However, no one has taken ownership of this responsibility, resulting in the outdated information.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

4. Assign responsibility for ensuring each NRC remote location maintains a consolidated inventory of all the IT system components located in that location, associated rack diagrams are kept up-to-date, and the inventory meets NRC requirements.

5. Create a consolidated inventory that meets NRC requirements of all the IT system components located in each NRC remote location.
6. Update the rack diagrams for each NRC remote location.

3.3 Plan of Action and Milestones (POA&M)

FISMA, OMB, and NIST define the requirements for a POA&M process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. In order to meet these requirements, NRC developed CSO-PROS-2016, *U.S. NRC POA&M Process*, and implemented an automated tool to help manage the agency POA&Ms. CSO-PROS-2016 describes the process for NRC to identify, assess, prioritize, and monitor the progress of corrective actions pertaining to security weaknesses and provides agency direction for the management and tracking of corrective efforts relative to known weaknesses in IT security controls. The automated tool ensures the agency's POA&M procedures are implemented consistently, completely, and accurately. However, the evaluation team found that NRC's POA&M process is not consistently followed and the agency's POA&M tool does not implement key OMB and NRC POA&M requirements. As a result, NRC's POA&Ms are not effective at monitoring the progress of corrective efforts relative to known weaknesses in IT security controls and therefore do not provide an accurate measure of security program effectiveness.

Finding #3: NRC POA&M Process Is Not Consistently Followed

CSO-PROS-2016 describes the process for NRC to identify, assess, prioritize, and monitor the progress of corrective actions pertaining to security weaknesses and provides agency direction for the management and tracking of corrective efforts relative to known weaknesses in IT security controls. However, the evaluation team found that NRC's POA&M process is not consistently followed. As a result, NRC's POA&Ms are not effective at monitoring the progress of corrective efforts relative to known weaknesses in IT security controls.

3.3.1 POA&M Process Requirements

CSO-PROS-2016 describes specific requirements for NRC POA&Ms, including the following:

- POA&Ms must be updated to add vulnerabilities as part of an independent assessment such as security testing and evaluation, continuous monitoring, vulnerability assessment report, security assessment report, security impact assessment, U.S. Government Accountability Office report, or OIG report. These weaknesses must be added to the POA&M as soon as possible, but not to exceed 60 days from the assessor's report.
- POA&Ms should be updated within the automated tool by the system owner with the most current information by the 15th of November, February, May, and August. System owners should keep abreast of weakness mitigation activities to ensure the documented status accurately reflects the environment at that particular point in time.
- Once the scheduled completion date is set, it should not be changed.

Instructions included with the annual IT security risk management activities memorandum, issued October 14, 2011, required system owners to add three risk management activities and respective due dates to their systems' POA&M in the agency information assurance tool and track them to completion. These activities are annual contingency plan testing, annual security control testing, and security-related document updates, including annual system security plan update.

3.3.2 Agency Has Not Fully Met Requirements

The evaluation team reviewed NRC POA&Ms for all four quarters of FY 2012. As in previous independent evaluations, we found that POA&Ms do not include all known security weaknesses and POA&Ms are not updated in a timely manner. We also found that scheduled completion dates are being changed and risk management activities are not added to POA&Ms as required.

POA&Ms Do Not Include All Known Security Weaknesses

CSO-PROS-2016 requires POA&Ms to be updated to add vulnerabilities identified as part of an independent assessment such as security testing and evaluation, continuous monitoring, vulnerability assessment report, security assessment report, security impact assessment, U.S. Government Accountability Office report, or OIG report. These weaknesses must be added to the POA&M as soon as possible, but not to exceed 60 days from the assessor's report. However, the evaluation team found some IT-related weaknesses were not added to the POA&Ms as required by agency policy.

- Weaknesses identified during the FY 2012 annual security control testing for four systems were not added to their respective POA&Ms.
- Recommendations from the FY 2012 contingency plan testing for five systems were not added to their respective POA&Ms.
- In July 2011, the OIG issued a report on NRC's shared "S" drive. None of the five recommendations from this report have been added to the appropriate POA&M.

POA&Ms Are Not Updated in a Timely Manner

CSO-PROS-2016 requires POA&Ms to be updated within the automated tool by the system owner with the most current information by the 15th of November, February, May, and August. The evaluation team found POA&Ms are not updated in a timely manner. The following are some examples of updates that are not timely:

- Approximately 24 percent of closed weaknesses were not reported closed in the quarter in which they were actually closed.
- Several weaknesses closed by the OIG almost a year ago have not been reported as closed on the POA&Ms, including 14 weaknesses from the regional reviews conducted in 2009.
- Approximately 12 percent of all weaknesses are being reported as on track when in fact they are delayed.

Scheduled Completion Dates Are Being Changed

CSO-PROS-2016 states that once the scheduled completion date is set, it should not be changed. However, the evaluation team found multiple instances of changed scheduled completion dates. In several instances, the dates were changed during or shortly after the transition from the manual POA&M process to the new automated tool, or when a previously closed weakness was reopened. As a result, weaknesses are being reported as on track when in fact they are actually delayed resulting in inaccurate reporting to OMB.

Risk Management Activities Are Not Added to POA&Ms

Instructions included with the annual IT security risk management activities memorandum required system owners to add annual contingency plan testing, annual security control testing, and security-related document updates, including annual system security plan update to their systems' POA&Ms. The evaluation team found that these activities were not added to POA&Ms for 7 of the agency's 22 systems.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

7. Provide refresher training to all staff responsible for implementing NRC's POA&M process.

Finding #4: POA&M Tool Does Not Consistently Implement Key OMB and NRC POA&M Requirements

As a result of recommendations from the FY 2007 FISMA independent evaluation, the agency implemented a tool for automating the POA&M process. The automated tool was put in place to ensure the agency's POA&M procedures are implemented consistently, completely, and accurately. However, the evaluation team found that the agency's POA&M tool does not implement key OMB and NRC POA&M requirements. As a result, NRC's POA&M process is not consistently implemented.

The following are some key OMB and NRC requirements for POA&M reporting:

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

The evaluation team reviewed NRC POA&Ms for all four quarters of FY 2012 and reviewed the POA&Ms in the agency's automated tool. The evaluation team found NRC's POA&M tool

allows weaknesses to be created that do not follow OMB and NRC POA&M requirements. Specifically, the tool:

- allows scheduled completion dates to be changed.
- allows weaknesses to be created without a scheduled completion date.
- allows weaknesses to be created with no value in the field that identifies the source of the weakness.
- allows a weakness to be closed without specifying an actual completion date.
- does not automatically change the status from on track to delayed once the scheduled completion date has passed.

The tool also allows users to enter actual completion dates in the future and allows users to enter an actual completion date when the status is not closed.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

8. Configure the agency's automated POA&M tool to do the following: (i) prevent scheduled completion dates from being changed, (ii) prevent weaknesses from being created without a scheduled completion date or weakness source, (iii) prevent weaknesses from being closed without specifying an actual date closed, (iv) prevent users from entering actual completion dates in the future, (v) prevent users from entering an actual completion date when the status is not closed, and (vi) automatically change the weakness status from on track to delayed once the scheduled completion date has passed.

3.4 Contingency Planning

FISMA and NIST require agencies to develop plans and procedures to ensure continuity of operations for information systems that support agency operations and assets. NRC has developed several types of plans that support these requirements, including the NRC COOP and information system contingency plans (ISCP). The evaluation team found that contingency planning for the NRC IT environment needs improvement. Specifically, the IT environment contingency plan does not address contingency events that do not require relocation to an alternate site, and procedures specific to contingency planning for NRC remote locations are not up-to-date. In addition, the COOPs for NRC remote locations that are referenced in the IT environment contingency plan are not current and only address situations where IT environment components at headquarters are not available.

3.4.1 Background

The NRC IT environment is a general support system that is located throughout NRC's headquarters campus buildings as well as at NRC remote locations. One of the remote locations has been designated as the alternate processing site for the NRC IT environment. The NRC IT environment is composed of several subsystems, including common computing services and

network infrastructure services. Common computing services are a client-server computing environment consisting of those services available to all NRC employees and contractors via the "NRC Network." There is one production file server in each NRC remote location as a part of this subsystem. Network infrastructure services are a distributed enterprise network consisting of a network infrastructure supporting interconnected subnets. All interconnected subnets facilitate internal and external office communications for NRC. The infrastructure is composed of NRC's headquarters campus local area network, NRC remote locations, and Resident Inspector sites. The IT environment contingency plan covers all of these components, even those located at NRC remote locations. The IT environment contingency plan also includes, as attachments, contingency plans for NRC-managed components located in NRC remote locations.

3.4.2 Contingency Planning Requirements and Definitions

Information system contingency planning normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency. Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management.

Organizational mission continuity applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. A COOP focuses on restoring an organization's mission essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP.

Disaster recovery plans apply to major, usually physical, disruptions to service that deny access to the primary facility infrastructure for an extended period. A disaster recovery plan is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. It may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. It may also support a business continuity plan or continuity of operations plan by recovering supporting systems for mission/business processes or mission essential functions at an alternate location.

Disaster recovery plans address only information system disruptions that require relocation. ISCPs differ from disaster recovery plans in that the ISCP procedures are developed for recovery of the system regardless of site or location. An ISCP can be activated at the system's current location or at an alternate site. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and system testing.

FINDING #5: Contingency Planning for the NRC IT Environment Needs Improvement

The evaluation team found that contingency planning for the NRC IT environment needs improvement. Specifically, the IT environment contingency plan does not address contingency events that do not require relocation to an alternate site, and procedures specific to contingency

planning for NRC remote locations are not up-to-date. In addition, the COOPs for NRC remote locations that are referenced in the IT environment contingency plan are not current and address only situations where IT environment components at headquarters are not available.

The NRC IT environment contingency plan provides steps required to recover the operation of IT environment components at the alternate processing site following a service disruption/emergency. The IT environment contingency plan does not describe restoring IT environment components using alternate equipment or performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions). For example, the contingency plan does not address contingency events that last less than 24 hours, such as the failure of a disk drive or power supply, or corruption of a database.

The evaluation team also found that contingency planning procedures specific to NRC remote locations are not up-to-date in the following ways:

1. The list of IT environment servers supporting NRC remote locations found in Appendix H of the IT environment contingency plan is not up-to-date.
2. The contingency plans for NRC remote locations that are attached to the IT environment contingency plan are not up-to-date and do not cover all NRC-managed servers in those locations. For example, the contingency plans for three NRC remote locations have not been updated to reflect the new addresses of locations that have moved in the past few years.
3. The IT environment contingency plan also does not include any contingency procedures for the IT environment and other IT components supporting one NRC remote location.

COOPs for NRC remote locations that are referenced in Appendix G of the IT environment contingency plan are out-of-date and refer only to situations where headquarters is unable to support IT environment components at the remote locations due to the destruction of the headquarters facility. These COOPs enable NRC staff in NRC remote locations to continue to use the enterprise e-mail system, remote access, and the Internet (and Internet E-mail). However; they do not address situations where the IT environment at an NRC remote location is unavailable for any reason. The IT environment contingency plan also does not include any COOP for the IT environment and other IT components supporting one NRC remote location.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

9. Update the IT environment contingency plan to include procedures for responding to short-term disruptions (those that last less than 24 hours), such as restoring components using alternate equipment or performing some or all of the affected business processes using alternate processing (manual) means.
10. Update the IT environment contingency plan to update contingency planning procedures specific to NRC remote locations that are not up-to-date. Specifically, update the list of IT environment servers supporting NRC remote locations that are referenced in Appendix

H of the IT environment contingency plan and update the contingency plans for NRC remote locations that are attached to the IT environment contingency plan.

11. Update the IT environment contingency plan to include contingency procedures for the IT environment and other IT components supporting the one NRC remote location for which these procedures are missing.
12. Update the COOPs for NRC remote locations that are referenced in Appendix G of the IT environment contingency plan to include current IT environment configurations at NRC remote locations and to address situations where the IT environment at those locations is unavailable for any reason.
13. Develop a COOP for the IT environment and other IT components supporting the one NRC remote location that does not have a COOP.

[Page intentionally left blank]

4 Consolidated List of Recommendations

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Update all procedures, guides, and user manuals that provide guidance for maintaining system inventory records within NSICD to clearly define which organization(s) are responsible for adding new system inventory records in NSICD.
2. Update the instructions included with the biannual inventory update to require system owners to notify the agency of any new systems that are not reflected in the data call.
3. Include all systems in NSICD, including all independent standalone hardware that has an NSICD system inventory number, in future biannual inventory update data calls.
4. Assign responsibility for ensuring each NRC remote location maintains a consolidated inventory of all the IT system components located in that location, associated rack diagrams are kept up-to-date, and the inventory meets NRC requirements.
5. Create a consolidated inventory that meets NRC requirements of all the IT system components located in each NRC remote location.
6. Update the rack diagrams for each NRC remote location.
7. Provide refresher training to all staff responsible for implementing NRC's POA&M process.
8. Configure the agency's automated POA&M tool to do the following: (i) prevent scheduled completion dates from being changed, (ii) prevent weaknesses from being created without a scheduled completion date or weakness source, (iii) prevent weaknesses from being closed without specifying an actual date closed, (iv) prevent users from entering actual completion dates in the future, (v) prevent users from entering an actual completion date when the status is not closed, and (vi) automatically change the weakness status from on track to delayed once the scheduled completion date has passed.
9. Update the IT environment contingency plan to include procedures for responding to short-term disruptions (those that last less than 24 hours), such as restoring components using alternate equipment or performing some or all of the affected business processes using alternate processing (manual) means.
10. Update the IT environment contingency plan to update contingency planning procedures specific to NRC remote locations that are not up-to-date. Specifically, update the list of IT environment servers supporting NRC remote locations that are referenced in Appendix H of the IT environment contingency plan and update the contingency plans for NRC remote locations that are attached to the IT environment contingency plan.
11. Update the IT environment contingency plan to include contingency procedures for the IT environment and other IT components supporting the one NRC remote location for which these procedures are missing.
12. Update the COOPs for NRC remote locations that are referenced in Appendix G of the IT environment contingency plan to include current IT environment configurations at NRC remote locations and to address situations where the IT environment at those locations is unavailable for any reason.
13. Develop a COOP for the IT environment and other IT components supporting the one NRC remote location that does not have a COOP.

[Page intentionally left blank]

5 Agency Comments

At an exit conference on November 1, 2012, agency officials agreed with the report's findings and recommendations. Subsequent to the exit conference, the agency provided informal comments, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

[Page intentionally left blank]

Appendix. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2012.

SCOPE

The evaluation focused on reviewing the agency's implementation of FISMA for FY 2012. The evaluation included an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines, and a review of information security policies, procedures, and practices of a representative subset of the agency's information systems, including contractor systems and systems provided by other Federal agencies. Three agency systems and one contractor system were selected for evaluation.

The evaluation was conducted at NRC headquarters from May 2012 through September 2012. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible. Throughout the evaluation, evaluators were aware of the potential for fraud, waste, or misuse in the program.

METHODOLOGY

Richard S. Carson & Associates, Inc., conducted an independent evaluation of NRC's implementation of FISMA for FY 2012. In addition to an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines, the evaluation included an assessment of the following topics specified in OMB's FY 2012 Inspector General FISMA Reporting Metrics.

- Continuous Monitoring Management.
- Configuration Management.
- Identity and Access Management.
- Incident Response and Reporting.
- Risk Management.
- Security Training.
- Plan of Action and Milestones.
- Remote Access Management.
- Contingency Planning.
- Contractor Systems.
- Security Capital 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, and to the 11 topics specified in OMB's reporting metrics.
- Security assessment and authorization documents for the four systems selected for evaluation during the FY 2012 independent evaluation, including security test and evaluation reports and vulnerability assessment reports prepared in support of security test and evaluation.
- Security categorizations, security plans, contingency plans, contingency plan test reports, and authorization to operate memoranda for all agency systems.
- Annual security control testing reports for all agency systems.
- Annual security control testing report for the agency's common controls, as controls such as incident response, security training, and security capital planning are partially provided at the agency level for all NRC information systems.

When reviewing security test and evaluation and annual security control testing reports, the team focused on security controls specific to the 11 topics specified in OMB's reporting metrics.

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

- NIST standards and guidelines.
- Management Directive and Handbook 12.5, *NRC Automated Information Security Program*.
- NRC Computer Security Office policies, processes, procedures, standards, and guidelines.
- NRC OIG audit guidance.

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