EVALUATION REPORT

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2013

OIG-14-A-03 November 22, 2013

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 22, 2013

MEMORANDUM TO: Mark A. Satorius
Executive Director for Operations

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

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2013 (OIG-14-A-03)

Attached is the Office of the Inspector General's (OIG) report titled *Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act [FISMA] for Fiscal Year 2013*. The objective was to perform an independent evaluation of the Nuclear Regulatory Commission's implementation of FISMA for FY 2013.

The report presents the results of the subject evaluation. The agency had no comments at the exit conference on November 19, 2013.

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 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 2013

Contract Number: GS-00F-0001N
Delivery Order Number: HHSP233201300215G

November 20, 2013

[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) 2013. This report presents the results of that independent evaluation. Carson Associates will also submit responses to the Office of Management and Budget's (OMB) annual FISMA reporting questions for OIGs via OMB's automated collection tool in accordance with OMB guidance.

OBJECTIVE

The objective was to perform an independent evaluation of NRC's implementation of FISMA for FY 2013.

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 2012 FISMA independent evaluation:

- The agency continued to maintain current authorizations to operate for all agency and contractor systems. In FY 2013, the agency completed security assessments and authorizations of seven systems. As of the completion of fieldwork for FY 2013, all 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 18 of the 21 agency systems and for both contractor systems.
- The agency completed annual security control testing for 15 agency systems and both contractor systems, and security test and evaluation in support of system authorization for 5 agency systems. The one system for which annual security control testing was not completed is scheduled to be decommissioned at the end of the calendar year, so no testing was required.
- The agency completed annual contingency plan testing for all agency and contractor systems, and updated the contingency plans for 17 agency systems and both contractor systems.
- The agency issued several updated documents, processes, and standards related to IT security including Management Directive and Handbook 12.5, *NRC Cyber*

Security Program; Agency-wide Rules of Behavior for Authorized Computer Use; Malicious Code Protection Guidance; Strong Password Standard; the NRC Information Security Program 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 agency's contractor system oversight program is not consistently implemented.
- There is a repeat finding from a previous FISMA evaluation: configuration management procedures are still not consistently implemented.
- There is a repeat finding from several previous FISMA evaluations: the NRC plan of action and milestone (POA&M) program still 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. Recommendations are made in this report for the new finding only. Recommendations for the repeat findings were made in prior reports, and completion of those findings is being tracked through the OIG followup process. A consolidated list of recommendations appears on page 15 of this report.

AGENCY COMMENTS

An exit conference was held with the agency on November 19, 2013. At this meeting, agency management stated their agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

ABBREVIATIONS AND ACRONYMS

ATO	Authorization to Operate
ATU	Authorization to Utilize
Carson Associates	Richard S. Carson and Associates, Inc.
CSO	Computer Security Office
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IT	Information Technology
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SP	Special Publication

[Page intentionally left blank]

TABLE OF CONTENTS

[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 program[2] 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-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated November 18, 2013, 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) 2013. 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. A consolidated list of recommendations appears on page 15.

2 Objective

The objective was to perform an independent evaluation of NRC's implementation of FISMA for FY 2013. The report appendix contains a description of the evaluation objective, scope, and methodology.

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 2012 FISMA independent evaluation:

[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.…"

- The agency continued to maintain current authorizations to operate for all agency and contractor systems. In FY 2013, the agency completed security assessments and authorizations of seven systems. As of the completion of fieldwork for FY 2013, all 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.[4]
- The agency completed or updated security plans for 18 of the 21 agency systems and for both contractor systems.
- The agency completed annual security control testing for 15 agency systems and both contractor systems, and security test and evaluation in support of system authorization for 5 agency systems. The one system for which annual security control testing was not completed is scheduled to be decommissioned at the end of the calendar year, so no testing was required.
- The agency completed annual contingency plan testing for all agency and contractor systems, and updated the contingency plans for 17 agency systems and both contractor systems.
- The agency issued several updated documents, processes, and standards related to IT security including Management Directive and Handbook 12.5, *NRC Cyber Security Program*; Agency-wide Rules of Behavior for Authorized Computer Use; Malicious Code Protection Guidance; Strong Password Standard; the NRC Information Security Program 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 agency's contractor system oversight program is not consistently implemented.
- There is a repeat finding from a previous FISMA evaluation: configuration management procedures are still not consistently implemented.
- There is a repeat finding from several previous FISMA evaluations: the NRC plan of action and milestone (POA&M) program still needs improvement.

Recommendations are made in this report for the new finding only. Recommendations for the repeat findings were made in prior reports, and completion of those findings is being tracked through the OIG followup process.

3.1 Contractor Systems Oversight

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

[4] Four operational NRC information systems are operating under an ATO extension.

or other organization on behalf of an agency. Management Directive and Handbook 12.5 requires Federal agencies or third-party service providers hosting NRC capabilities to meet NRC cyber security requirements. Computer Security Office (CSO) process CSO-PROS-2030, *NRC Risk Management Framework (RMF) and Authorization Process*, provides the process for applying the RMF described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, to secure NRC systems, including contractor systems, and includes the steps required to obtain IT system authorization and authorization requirements for IT systems, applications, laptops, services, and facilities.

However, the FISMA evaluation team found that agency's contractor system oversight program is not consistently implemented. Specifically, NRC's inventory of contractor systems is incomplete and the NRC's RMF is not consistently followed for contractor systems. As a result, the agency cannot determine whether systems that are owned or operated by contractors or other entities are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Finding #1: NRC's Inventory of Contractor Systems Is Incomplete

CSO-PROS-2030 provides the process for applying the NIST RMF secure NRC systems and defines the six types of systems and services to which the RMF applies. However, the FISMA evaluation team found that NRC's inventory of contractor systems is incomplete. As a result, NRC is not able to obtain assurance that security controls of such systems and services are effectively implemented and comply with Federal and agency guidelines.

3.1.1 NRC Inventory Requirements

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

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

The NRC inventory also identifies the owner of the system (e.g., NRC or Contractor), the security type of the system (e.g., Major Application, General Support System, Listed System, Other System), and whether or not the system is an e-Government system (i.e., operated by another Federal agency).

3.1.2 Inventory Information for NRC Contractor Systems Is Inconsistent

The FISMA evaluation team reviewed the NRC inventory as of September 30, 2013, and found several examples of incorrect or missing information for NRC contractor systems. The following are some examples:

- Seven systems are missing an owner (i.e., NRC or Contractor). Based on other information in the inventory, these are likely Contractor systems.
- Four systems are missing a security type (i.e., Major Application, General Support System, Listed System, Other System).
- Eight systems are missing the flag denoting whether the system is an e-Government system.
- Two systems are incorrectly classified as IT Systems when they should be Services.
- Three systems are incorrectly classified as Applications when they should be either IT Systems or Services.
- One system is incorrectly classified as a Service when it should be classified as Social Media.
- The inventory is missing a Federal data center that hosts an IT System.

RECOMMENDATION

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

1. Update the information in the NRC inventory for contractor systems to include missing information and to correctly classify contractor systems in accordance with CSO-PROS-2030, *NRC Risk Management Framework*.

Finding #2: NRC's RMF Is Not Consistently Followed for Contractor Systems

CSO-PROS-2030 describes the process for applying the NIST RMF to secure NRC systems, including the steps required to obtain IT system authorization and authorization requirements for IT systems, applications, laptops, services, and facilities. However, the FISMA evaluation team found that NRC's RMF is not consistently followed for contractor systems. This is likely due in

part to the fact that the inventory of contractor systems is incomplete. As a result, NRC is not able to obtain assurance that security controls of such systems and services are effectively implemented and comply with Federal and agency guidelines.

3.1.3 NRC RMF Requirements for Contractor Systems

CSO-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.

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. Instructions included with the IT security risk management activities memorandum for FY 2013, issued November 28, 2012, included a requirement to ensure systems owned and/or operated by other agencies or contractors also satisfy annual contingency plan testing and control testing requirements and have a valid ATO. For such systems, the NRC organization must obtain a memorandum from the agency that owns or operates the system confirming the following:

- Completion of annual contingency plan testing, including date test was completed.
- Completion of annual control testing, including date test was completed.
- Status of ATO, including the date of the current ATO. For new or revised ATO dates, also provide the agency's certification/security control assessment and ATO memos.

This memorandum was required to be entered in the agency's official document repository and submitted to the CSO by emailing the document's repository tracking number by September 15, 2013.

3.1.4 Agency Has Not Fully Met Requirements

The FISMA evaluation team reviewed the authorization documentation for contractor systems and found that the agency has not fully met NRC RMF requirements for contractor systems. The following are some examples:

- The evaluation team identified one system on the inventory classified as an IT System that does not have an ATO, as well as one system that may be incorrectly classified as an Application.
- The IT security risk management activities memorandum and instructions for FY 2013 listed nine systems to which annual requirements for systems owned and/or operated by other agencies or contractors apply, one of which was retired after the memorandum was issued. However, the evaluation team found that the list of contractor systems in the November 2012 memorandum was incomplete. The list should have included three additional systems, one of which has had an ATU since 2011, as well as one additional system that may be incorrectly classified as an Application. In addition, the evaluation team found that for the systems on the list, the agency did not obtain the required documentation from the hosting organization(s) as required. Required documentation was submitted only for one system.
- For Services not authorized by another Federal agency, they must be authorized to operate by the agency as an IT System. The evaluation team identified four systems on the inventory classified as a Service that are not authorized by another Federal agency and do not have an ATO issued by NRC.

RECOMMENDATIONS

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

2. Based on the updated inventory of contractor systems, identify those that are not compliant with CSO-PROS-2030, *NRC Risk Management Framework*, and complete appropriate authorization activities for those systems.
3. 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.

3.2 Configuration Management

FISMA requires agencies to develop policies and procedures that ensure compliance with minimally acceptable system configuration requirements as determined by the agency. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, requires organizations to (1) develop, document, and maintain under configuration control, a current baseline configuration for information systems; (2) establish and document mandatory configuration settings for IT products employed within information systems; (3) monitor and control changes to the configuration settings; (4) scan for vulnerabilities in information systems; (5) remediate legitimate vulnerabilities within organization-defined response times; and (6) incorporate flaw remediation into the configuration management process.

The agency has established and is maintaining a configuration management program that is consistent with FISMA requirements and applicable NIST guidelines. The FY 2011 FISMA evaluation found that configuration management procedures are not consistently implemented. Specifically, (i) standard baseline configurations are not implemented on some NRC systems; (ii) software compliance assessment procedures are not consistently implemented; and (iii)

vulnerability remediation and patch management procedures are not consistently implemented. The agency has yet to implement the five recommendations from the FY 2011 FISMA evaluation related to configuration management and many of the same issues were found again in the FY 2013 evaluation. As a result, information security protections may not be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of NRC information and information systems.

Finding #3: NRC Configuration Management Procedures Are Not Consistently Implemented

The NRC configuration program includes CSO issued processes, procedures, standards, guidelines, checklists, and templates. These include standard baseline configurations for software, hardware, and other technologies in use at the agency; procedures for assessing software for compliance with baseline configurations; and processes for timely remediation of vulnerabilities, including configuration-related vulnerabilities and scan findings, and for the timely and secure installation of software patches. However, the FISMA evaluation team found that NRC configuration management procedures are not consistently implemented. Specifically, (i) standard baseline configurations are not implemented on some NRC systems; (ii) software compliance assessment procedures are not consistently implemented; and (iii) vulnerability remediation and patch management procedures are not consistently implemented. As a result, information security protections may not be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of NRC information and information systems.

3.2.1 Configuration Management Requirements

Standard Baseline Configurations

CSO is responsible for identifying system configuration standards to be used in the protection of any information system that stores, transmits/receives, or processes NRC information. CSO publishes and maintains NRC-specific configuration standards, but also relies on those published by other authoritative sources. The precedence for the applicability of configuration baselines is CSO Standards; Defense Information Systems Agency finalized standards, checklists, and guidance; and Center for Internet Security finalized benchmarks.

The CSO has developed five broad categories of standards:

- **General Cyber Security Standards** – technology/implementation independent requirements that apply across the NRC and to all information systems that store, transmit/receive, or process NRC information. These standards include CSO-STD-0001, *NRC Strong Password Standard*, and CSO-STD-0020, *Organization Defined Values for System Security Controls*.
- **Network Standards** –apply to the network infrastructure overall, as well as minimum baseline cyber security requirements for network devices, such as network routers, switches, firewalls, and wireless network components that transmit/receive NRC information.

- **Operating System Standards** –apply to operating systems for all types of computers except firmware and operating systems for network devices (e.g., routers, firewalls, switches, sensors, and load balancers). Standards for network device operating systems are included within the Network Standards category.
- **Application Standards** –apply to application software used to perform a specific task, such as word processing, Web browsing, financial management, and software used to manage or provide services to the infrastructure (e.g., database, e-mail, file, and Web server). Internet applications (e.g., Twitter, Facebook, Flickr, WordPress, and YouTube) are covered under the CSO-STD-1314, *NRC Web 2.0 Implementation Standard*.
- **Device Standards** –apply to IT resources that store, process, and print NRC information.

Software Compliance Assessment

CSO-PROS-2030 requires vulnerability assessments as part of Step 4 of the RMF. CSO-PROS-1323, *U.S. NRC Agency-wide Continuous Monitoring Program*, requires networked-based scans, hardening checks, Web application security assessments for Web-based systems, and wireless scans, on an at least annual basis, if not more frequently depending on the system sensitivity level. System owners must provide evidence of periodic scanning to the CSO. CSO-STD-0020 requires system owners to scan for vulnerabilities at least quarterly. CSO-PROS-1401, *Periodic System Scanning Process*, describes the process to be used to effectively perform periodic scans on NRC systems.

The IT security risk management activities memorandum and instructions for FY 2013 define the frequency for performing patch vulnerability management activities. System Owners must complete the following to continuously detect and resolve vulnerabilities in their systems:

- Track patch and vulnerability management through a formal change control process.
- Establish a schedule for patching and system vulnerability scanning that is aligned to resolve vulnerabilities and verify fixes.
- Ensure routine scans and security checks are conducted in a timely fashion.
- Ensure findings identified in the scans and security checks are added and tracked in the POA&M in accordance with CSO-PROS-2016, *U.S. NRC POA&M Process*.
- Upload a Periodic Scan Report as an artifact in the agency information assurance tool to serve as evidence of scanning and patching/lack of patching. The CSO will review the previous report when verifying the current quarter's POA&M.

Vulnerability Remediation and Patch Management

CSO-STD-0020 requires legitimate vulnerabilities to be remediated in accordance with an organizational assessment of risk and within the following timeframes:

- Within 21 calendar days for critical findings.
- Within 45 calendar days for high-risk findings.
- Within 90 calendar days for moderate-risk findings.

- Within 120 calendar days for low-risk findings.

NRC also requires system owners to ensure automated mechanisms are employed quarterly to determine the state of information system components with regard to flaw remediation. The IT security risk management activities memorandum and instructions for FY 2013 require system owners to patch, scan, and check the security of their systems with the rigor and frequency appropriate for the system sensitivity level and define the frequency for conducting routine patching.

3.2.2 Agency Has Not Fully Met Requirements

The FISMA evaluation team reviewed the security test and evaluation results for the four systems selected for evaluation in FY 2013, and the annual security control test results for agency and contractor systems, specifically test results for controls related to configuration management, vulnerability scanning, and patching. We also reviewed a network security evaluation report for an assessment performed on the NRC network by another agency in the spring of 2012. As in previous years, we found that configuration management continues to be an issue with many NRC systems.

Standard Baseline Configurations Are Not Implemented on Some NRC Systems

As reported in the FY 2011 FISMA evaluation, the FY 2013 FISMA evaluation team found that standard baseline configurations are not implemented on some NRC systems. Vulnerability scanning performed as part of security control assessment activities identified numerous vulnerabilities that demonstrate non-compliance with required baseline configurations in more than half of NRC's operational systems. These are vulnerabilities that have been identified by the agency as actual weaknesses requiring remediation and most are being tracked on the agency's POA&Ms. This issue is due in part to problems with the templates used in the agency's compliance assessment tool. Recent security control assessments performed by the agency found that some compliance tool templates are not configured per NRC established checklists. As a result, security controls are not being assessed against the correct criteria. In addition, recent security control assessments performed by the agency found issues with group policy objects issued by the agency's infrastructure system not matching NRC-mandated configuration settings. As a result, any server applying these group policy objects are not compliant. The 2012 security evaluation performed by another agency on the NRC network also found a lack of a strictly enforced software baseline for Windows servers.

Software Compliance Assessment Procedures Are Not Consistently Implemented

As reported in the FY 2011 FISMA evaluation, the FY 2013 FISMA evaluation team found that software compliance assessment procedures are not consistently implemented. Recent security control assessments performed by the agency found that four of NRC's operational systems continue to have issues implementing software compliance assessment procedures in accordance with NRC requirements. These systems are not performing scans in accordance with agency timeframes. In one instance, a portion of a system's components were not being scanned at all. For another system, a deviation was granted for a portion of the system to be scanned annually

instead of quarterly; however, scans were not performed in accordance with the timeframe in the approved deviation. The most significant finding from recent security control assessments performed by the agency is that multiple components of the NRC's infrastructure system are not being scanned because they were just not included in scans, were not joined to the domain, or credentials were not used to scan certain components as required. For the fourth system, scans are not being performed quarterly as required.

Vulnerability Remediation and Patch Management Procedures Are Not Consistently Implemented

As reported in the FY 2011 FISMA evaluation, the FY 2013 FISMA evaluation team found that configuration-related vulnerabilities, scan findings, and security patch-related vulnerabilities are not always remediated in a timely manner. Recent security control assessments performed by the agency found that one-third of NRC's operational systems continue to have issues remediating vulnerabilities in a timely manner. Delays in patching systems were due in part to problems the agency was having with their patch management software. The software was unable to push patches to some system components for 2 months, or was dropping servers from the group to receive a particular patch. As a result, servers for two systems were not consistently receiving the required patches. In addition, recent security control assessments performed by the agency found another nine systems with either missing patches and/or outstanding weaknesses from previous assessments. The 2012 security evaluation performed by another agency on the NRC network also found systematic issues with patching UNIX systems throughout the agency, issues with patching third-party software running on Windows servers, and issues with patching database software.

RECOMMENDATIONS

The issue with configuration management procedures is a repeat finding from the FY 2011 FISMA evaluation. The five recommendations from the FY 2011 FISMA evaluation are still open, as the agency has not completed all of their planned remediation activities. Therefore, OIG is not issuing any new recommendations for addressing this finding.

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. 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. NRC uses an automated tool for tracking IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency. The FY 2012 FISMA evaluation found that NRC's POA&M process was not consistently followed and the agency's POA&M tool did not implement key OMB and NRC POA&M requirements.

The agency has yet to complete the two recommendations from the FY 2012 FISMA evaluation related to the POA&M process and many of the same issues were found again in FY 2013. As a result, NRC's POA&Ms are still 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 #4: NRC POA&M Program Still Needs Improvement

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. As a result of recommendations from the FY 2007 FISMA 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 FY 2013 FISMA evaluation team found that NRC's POA&M program still needs improvement. Specifically, NRC's POA&M process is still not consistently followed and the agency's POA&M tool still does not implement key OMB and NRC POA&M requirements. The evaluation team also found that initial target remediation dates are frequently missed. As a result, the 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 IT security risk management activities memorandum for FY 2013 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.

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.

3.3.2 Agency Has Not Fully Met Requirements

The FISMA evaluation team reviewed NRC POA&Ms for all four quarters of FY 2012. As in previous FISMA evaluations, we found that POA&Ms do not include all known security weaknesses and POA&Ms are not updated in a timely manner.

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, as reported in the FY 2012 FISMA evaluation, the FY 2013 FISMA evaluation team found some IT-related weaknesses were not added to the POA&Ms as required by agency policy.

- Weaknesses identified during the agency's 2013 annual security control testing for two systems were not added to their respective POA&Ms.
- Recommendations from the agency's 2013 contingency plan testing for seven systems were not added to their respective POA&Ms.
- The FY 2012 FISMA evaluation noted that recommendations from an OIG report issued in July 2011 on NRC's shared "S" drive had not been added to the appropriate POA&M. To date, they still have not been added to the POA&M and three of the recommendations are still open.
- Between August 2012 and January 2013, OIG issued five reports on information security risk evaluations performed in the regional offices and at the Technical Training Center. None of the recommendations from these reports have been added to the appropriate POA&M.
- Only 2 of the 13 recommendations from the FY 2012 FISMA evaluation have been added to the appropriate POA&M.
- In January 2013, OIG issued a report on the use and security of social media. The report included 34 recommendations, of which 8 were IT security related; however, none were added to the appropriate POA&M.
- In April 2013, OIG issued a report on one of the agency's systems. The report included seven recommendations, of which two were IT security related; however, they were not added to the POA&M for the system.

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. Instructions included with the IT security risk management activities memorandum for FY 2013 required system owners to add annual contingency plan testing, annual security control testing, and security-related document updates, including annual system security plan updates to their systems' POA&Ms.

As reported in the FY 2012 FISMA evaluation, the FY 2013 FISMA evaluation team found POA&Ms are not updated in a timely manner. The following are some examples of updates that are not timely:

- Approximately 14 percent of closed weaknesses were not reported closed in the quarter in which they were actually closed.
- Weaknesses closed by OIG are still not being reported as closed on the POA&Ms.
- The program level POA&M and eight system POA&Ms still include weaknesses that are more than 1 year old. One system POA&M has more than 300 weaknesses that are more than 1 year old and should no longer be reported.
- The evaluation team found that some or all of the annual IT security risk management activities were not added to POA&Ms for 6 of the agency's 23 systems. This is a repeat finding for four of those systems.

3.3.3 NRC's POA&M Tool Still Does Not Implement Key OMB and NRC POA&M Requirements

In the FY 2012 FISMA evaluation, 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. These two issues have been corrected in a new version of the tool currently under evaluation and testing; however, the remaining issues have yet to be addressed.

3.3.4 Initial Target Remediation Dates Are Frequently Missed

The agency's progress in correcting weaknesses reported on its POA&Ms has declined since FY 2012. In FY 2012, the agency closed 30 percent of its program level weaknesses and 55 percent of its system level weaknesses. However, in FY 2013, the agency closed only 15 percent of its program level weaknesses and 37 percent of its system level weaknesses.

RECOMMENDATIONS

The issue with the NRC POA&M program is a repeat finding from the FY 2012 FISMA evaluation. The two recommendations from the FY 2012 FISMA evaluation are still open, as the agency has not completed all of their planned remediation activities. Therefore, OIG is not issuing any new recommendations for addressing this finding.

4 Consolidated List of Recommendations

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

1. Update the information in the NRC inventory for contractor systems to include missing information and to correctly classify contractor systems in accordance with CSO-PROS-2030, *NRC Risk Management Framework*.
2. Based on the updated inventory of contractor systems, identify those that are not compliant with CSO-PROS-2030, *NRC Risk Management Framework*, and complete appropriate authorization activities for those systems.
3. 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.

[Page intentionally left blank]

5 Agency Comments

An exit conference was held with the agency on November 19, 2013. At this meeting, agency management stated their agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

[Page intentionally left blank]

Appendix. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective was to perform an independent evaluation of NRC's implementation of FISMA for FY 2013.

SCOPE

The evaluation focused on reviewing the agency's implementation of FISMA for FY 2013. 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 June 2013 through September 2013. 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 2013. 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 2013 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 2013 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 Cyber 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, from Richard S. Carson & Associates, Inc.

Report Location: G:AUDIT\14-A-03 FISMA\FINAL EVALUATION REPORT – OIG-14-A-03 Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2013 (PXB).docx

Distribution
AIGA r/r
MBlair
JGordon
BSerepca
SZane
SDingbaum

ADAMS Accession Number:

OIG	OIG	OIG	OIG	OIG	OIG	OIG
MBlair	JGordon	BSerepca	SZane	SDingbaum	DLee	HBell
11/ /13	11/ /13	11/ /13	11/ /13	11/ /13	11/ /13	11/ /13

SUNSI Review - OK for Public Release	**SUNSI Review – Redacted for Public Release**	**SUNSI Review – OUO Not for Public Release**
SZane	SZane	SZane
11/ /13	11/ /13	11/ /13

OFFICIAL FILE COPY