Office of the Inspector General

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

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

OIG-15-A-02
November 13, 2014

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 13, 2014

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 2014 (OIG-15-A-02)

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 2014*. The purpose of this evaluation was to perform an independent evaluation of NRC's implementation of FISMA for Fiscal Year 2014.

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

- Continuous monitoring is not performed as required.
- There is a repeat finding from previous FISMA evaluations: configuration management procedures are still not consistently implemented.
- There is a repeat finding from several previous FISMA evaluations: plan of action and milestone management still needs improvement.

This report presents the results of the subject evaluation and contains a recommendation to improve the agency's implementation of FISMA. Following the November 13, 2014, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

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

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

Attachment: As stated

Office of the Inspector General

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

OIG-15-A-02

November 13, 2014

Results in Brief

Why We Did This Review

The Federal Information Security Management Act (FISMA) of 2002 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of 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. The Office of Management and Budget (OMB) requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

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

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

What We Found

NRC has continued to make improvements in its information technology security program and progress in implementing the recommendations resulting from previous FISMA evaluations. However, we found that continuous monitoring is not performed as required. Specifically, we found that annual risk management activities in support of continuous monitoring were either delayed or not performed at all. In addition, system security plans, including the NRC Information Security Program Plan (ISPP), were not updated to reflect changes to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, with the issuance of Revision 4 in April 2013. As a result, NRC cannot ensure the effectiveness of information security controls for NRC systems and cannot identify and control risk.

We also identified two repeat findings from previous FISMA evaluations. We found that configuration management procedures are still not consistently implemented and plans of action and milestone management still needs improvement.

What We Recommend

To improve the agency's implementation of FISMA, we make a recommendation to develop a plan and schedule for updating system security plans, as well as the ISPP, to reflect NIST SP 800-53, Revision 4. Recommendations for the repeat findings were made in prior reports, and completion of these findings is being tracked through the OIG followup process.

Management stated their general agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

APPENDIX

ABBREVIATIONS AND ACRONYMS

ATO	Authorization to Operate
ATO-CA	Continuous ATO
CP	Contingency Plan
CSO	Computer Security Office
FISMA	Federal Information Security Management Act
FY	Fiscal Year
ISPP	Information Security Program Plan
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

I. 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, and OMB M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, require OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

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

[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 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…."

submit responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool in accordance with OMB guidance.

II. OBJECTIVE

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

III. FINDINGS

NRC has continued to make improvements to its information technology (IT) security program and progress in implementing the recommendations resulting from previous FISMA evaluations. The agency has accomplished the following since the FY 2013 FISMA independent evaluation:

- The agency continued to maintain current authorizations to operate for most agency and contractor systems. In FY 2014, the agency completed security assessments and authorizations of two systems. As of the completion of fieldwork for FY 2014, 20 of the 22 operational information systems had a current authorization to operate (ATO).[4] Two systems are operating without a current ATO as their ATO extensions have expired.

- The agency completed or updated security plans for 19 of the 21 operational information systems.

- The agency completed annual security control testing for 14 operational information systems, and security control assessment in support of system authorization for 2 agency systems.

- The agency completed annual contingency plan testing for 17 operational information systems.

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

- The agency updated the contingency plans for 14 operational information systems.

- The agency issued several new or updated documents, processes, and standards related to IT security including Enterprise Risk Management Program Plan, Authority to Use Process, IT System Decommissioning and Disposal Process, Endpoint Protection Security Standard, Network Infrastructure Standard, and Microsoft Internet Explorer 9 Configuration Standard.

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 IT security program weaknesses:

- Continuous monitoring is not performed as required.

- There is a repeat finding from previous FISMA evaluations: configuration management procedures are still not consistently implemented.

- There is a repeat finding from several previous FISMA evaluations: plan of action and milestone (POA&M) management still needs improvement.

Recommendations are made in this report for the new finding concerning continuous monitoring 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. Continuous Monitoring Is Not Performed as Required

Step 6 of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), ongoing or continuous monitoring, is a critical part of organization-wide risk management. A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. For systems operating under a continuous ATO (ATO-CA), continuous monitoring is essential for determining risk associated with systems and for ensuring risk-based decisions are made concerning continued system operation.

Computer Security Office (CSO) process CSO-PROS-1323, *U.S. NRC Agency-wide Continuous Monitoring Program*, provides direction for NRC continuous monitoring activities and requires a set of NRC core controls to be tested during annual security control testing due to their criticality and potential for being modified by system changes. Due to a delay in awarding the new agencywide cyber security support contract, some of the required continuous monitoring activities have not been performed. As a result, NRC cannot ensure the effectiveness of information security controls for NRC systems and cannot identify and control risk.

What Is Required

Federal Guidance Regarding Continuous Monitoring

FISMA requires that agencies establish a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct security control assessments at a frequency depending on risk, but no less than annually. FISMA also mandates that agencies follow NIST standards and guidelines to establish and secure that framework.

NIST Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Step 6 of the RMF, ongoing or continuous monitoring, is a critical part of that risk management process.

Key activities performed during Step 6 include the following:

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

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

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

Internal Guidance Regarding Continuous Monitoring

NRC Continuous Monitoring Program

CSO-PROS-1323 provides direction for NRC continuous monitoring activities and describes the process for annual continuous monitoring reviews, related roles, and responsibilities, and evaluation criteria. It requires a set of NRC core controls to be tested during annual security control testing due to their criticality and potential for being modified by system changes.

Each year, the agency Executive Director for Operations issues a memorandum requiring system owners to perform risk management activities required for FISMA. The purpose of these activities is to identify and control risk, and permit continuous improvement of the agency's cybersecurity risk posture. All testing activities must be completed and the final test reports dated within 1 year of the previous test report date. The memorandum includes a table listing critical dates for completing these activities.

In the FY 2014 memorandum, system owners were required to take the following actions:

- Perform an Annual Security Control and Vulnerability Test.
- Perform an annual Contingency Plan (CP) test and complete an updated CP, CP Test Plan, and CP Test Report.
- Update all security-related documentation (e.g., System Security Plan, Security Risk Assessment, POA&M). System security plans and POA&Ms must be reviewed at least quarterly.

Continuous Monitoring for Systems Issued an ATO-CA

NRC is transitioning to a continuous authorization process and has implemented a policy that requires a full system authorization process be completed prior to the system entering into a continuous authorization state. The NRC Designated Approving Authority accepts the risk of operating the system in a continuing authorization state and requires use of continuous monitoring processes to determine risks associated with the system and ensure risk-based decisions are made concerning continued system operation. Systems issued an ATO-CA must follow the instructions in the annual risk management activities memorandum, and use the security impact analysis process for system changes.

NRC Information Security Program Plan

The NRC Information Security Program Plan (ISPP) provides an overview of the security requirements for the NRC-wide information security program and describes the program management and common controls in place or planned for meeting those requirements. Annual review and approval of the ISPP is scheduled just after the ISPP annual security control test is completed to ensure those results are included in the annual update.

What We Found

Noncompliance With Continuous Monitoring Guidance

Figure 1 below summarizes the required continuous monitoring activities that were not performed by the agency in FY 2014. For the system with the expired ATO, February 2013 was the last annual security control test, November 2012 was the last contingency plan test, July 2012 was the last contingency plan update, and March 2013 was the last security plan update.

Figure 1:

Required Activity	# Non-Compliant Systems	Security Categorization	ATO Status
Annual Security Control Testing	6	High: 3 Moderate: 3	ATO: 2 ATO-CA: 3 Expired ATO: 1
Annual Contingency Plan Testing	5	High: 2 Moderate: 3	ATO-CA: 4 Expired ATO: 1
Annual Contingency Plan Update	8 (3 not updated since 2012)	High: 1 Moderate: 7	ATO: 3 ATO-CA: 3 ATO-Extension: 1 Expired ATO: 1
Annual Security Plan Update	3	High: 1 Moderate: 2	ATO: 1 ATO-CA: 1 Expired ATO: 1

Source: OIG

Annual Security Control Assessments Were Delayed

Of the 16 systems that had an annual security control assessment completed in FY 2014, only 5 were completed within 1 year of the previous year’s testing.

System Security Plans Were Not Updated To Be Compliant with NIST SP 800-53 Revision 4

In April 2013, NIST issued SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Agencies have 1 year from the publication date of a revision to a standard to comply with the new standard. None of the system security plans updated after April 2014 were updated to include changes to NIST SP 800-53.

NRC Information Security Program Plan Has Not Been Updated

The NRC ISPP is reviewed and updated after annual security control testing has been performed on the NRC common controls. The NRC common controls were last tested in the fall of 2013, but the ISPP was last updated March 2013. The ISPP does not reflect changes to NIST SP 800-53 with the issuance of Revision 4 in April 2013.

Why This Occurred

Delays in Awarding the Cyber Security Support Contract

On March 24, 2014, the CSO notified the NRC Designated Approving Authorities that some required continuous monitoring activities are delayed due to a delay in awarding the new agencywide cyber security support contract. The memorandum identified which systems would not meet their due dates for annual security control testing and contingency plan testing and update. The CSO indicated that the increased risk due to the delays does not present a significant increase in risk to NRC. The majority of the delays identified during the FY 2014 evaluation were not discussed in the March 2014 memorandum. The agency did not provide documentation explaining why other continuous monitoring activities not mentioned in the memorandum were not performed as required.

Why This Is Important

NRC Cannot Ensure Effectiveness of Security Controls

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. For systems operating under an ATO-CA, continuous monitoring is essential for determining risk associated with systems and for ensuring risk-based decisions are made concerning continued system operation. If continuous monitoring activities are not performed as required, NRC cannot ensure the effectiveness of the information security controls for NRC systems and cannot identify and control risk.

Recommendation

OIG recommends that the Executive Director for Operations

1. In support of continuous monitoring, develop a plan and schedule for updating all NRC system security plans, as well as the NRC Information Security Program Plan, to reflect NIST SP 800-53, Revision 4.

B. NRC Configuration Management Procedures Are Not Consistently Implemented

FISMA requires agencies to develop policies and procedures that ensure compliance with minimally acceptable system configuration requirements as determined by the agency. 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. As in previous FISMA evaluations, the FY 2014 FISMA evaluation team 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 three of 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 and FY 2014 evaluations. 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.

What Is Required

Federal Guidance Regarding 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 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.

Internal Guidance Regarding Configuration Management

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.

Software Compliance Assessment

CSO-PROS-2030, *NRC Risk Management Framework and Authorization Process*, requires vulnerability assessments as part of Step 4 of the RMF. CSO-PROS-1323 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, *Organization Defined Values for System Security Controls*, requires system owners to scan for vulnerabilities at least quarterly. CSO-PROS-1401, *Periodic System Scanning Proces*s, describes the process to be used to perform periodic scans on NRC systems.

The IT security risk management activities memorandum and instructions for FY 2014 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.

- Document the results of vulnerability assessment testing in a system Periodic Scan Report in accordance with CSO-PROS-1401 and ensure the report is uploaded into the agency information assurance tool.

- Ensure weaknesses identified through testing are incorporated into the system's POA&M in accordance with CSO-PROS-2016, *U.S. NRC POA&M Process*.

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 2014 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.

What We Found

Noncompliance With Configuration Management Guidance

The FISMA evaluation team reviewed the security test and evaluation results for the four systems selected for evaluation in FY 2014, 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. As in previous years, the FISMA evaluation team 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 previous FISMA evaluations, the FY 2014 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 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.

Software Compliance Assessment Procedures Are Not Consistently Implemented

As reported in previous FISMA evaluations, the FY 2014 FISMA evaluation team found that software compliance assessment procedures are not consistently implemented. Recent security control assessments performed by the agency found that for one system, scans are not being performed quarterly as required.

Vulnerability Remediation and Patch Management Procedures Are Not Consistently Implemented

As reported in previous FISMA evaluations, the FY 2014 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 half of NRC's operational systems continue to have issues remediating vulnerabilities in a timely manner.

Why This Occurred

Corrective Actions From Previous FISMA Evaluations Have Not Been Completed

The agency has yet to complete the three of the five recommendations from the FY 2011 FISMA evaluation related to configuration management and many of the same issues were found again in FY 2013 and FY 2014.

Why This Is Important

Information Security Protections May Not Be Commensurate With Risk

The configuration of an information system and its components has a direct impact on the security posture of the system. System changes can adversely impact the previously established security posture; therefore, effective configuration management is vital to the establishment and maintenance of security of information and the information system. If configuration management procedures are not consistently implemented, 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.

Recommendation

The issue with configuration management procedures is a repeat finding from the FY 2011 and FY 2013 FISMA evaluations. Three of 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.

C. POA&M Management Needs Improvement

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. NRC developed CSO-PROS-2016, 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. As in several previous FISMA evaluations, the FY 2014 FISMA evaluation team 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 and FY 2014. 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.

What Is Required

Federal and Internal POA&M Guidance

Federal POA&M Guidance

FISMA requires agencies to develop, document, and implement a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.

NIST requires organizations to implement a process for ensuring POA&Ms, for both the security program and associated organizational information systems, are maintained and document remedial security actions to mitigate risk. Organizations must develop a POA&M for each information system to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. Organizations are required to update POA&Ms on an organization-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Key OMB POA&M reporting requirements include the following:

- 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.

Internal POA&M Guidance

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 2014 required system owners to add 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 quarterly system security plan review and update.

What We Found

Noncompliance With POA&M Guidance

POA&Ms Do Not Include All Known Security Weaknesses

As reported in several previous FISMA evaluations, the FY 2014 FISMA evaluation team found some IT-related weaknesses were not added to the POA&Ms as required by agency policy.

- Some weaknesses identified during the agency's 2014 annual security control testing for two systems were not added to their respective POA&Ms.

- Recommendations from the agency's 2014 contingency plan testing for three 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 two 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. Recommendations from four of these reports were never added to the appropriate POA&M (all of their recommendations have been closed). Recommendations from one of these reports were not added to the appropriate POA&M until the third quarter of FY 2014, over 18 months after the report was issued.

- Nine of the 13 recommendations from the FY 2012 FISMA evaluation were not added to the appropriate POA&M until the third quarter of FY 2014, over 18 months after the report was issued.

- 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 have been added to the appropriate POA&M.

- OIG-13-A-16, Audit of NRC's Safeguards Information Local Area Network and Electronic Safe, issued April 1, 2013, included seven recommendations, of which two were IT security related; however, they were not added to the POA&M for the system. The recommendations were finally added to the agency's program level POA&M in the third quarter of FY 2014, over 1 year after the report was issued.

- Recommendations from the FY 2013 FISMA independent evaluation have not been added to the appropriate POA&M.

POA&Ms Are Not Updated in a Timely Manner

As reported in several previous FISMA evaluations, the FY 2014 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 10 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 17 system POA&Ms still include over 730 weaknesses combined that are more than 1 year old.

One system POA&M has more than 340 weaknesses that are more than 1 year old and should no longer be reported. OMB guidance[5] states that weaknesses that are no longer undergoing correction and have been completely mitigated for over a year should no longer be reported in the agency POA&Ms.

- The evaluation team found that some or all of the annual IT security risk management activities were not added to POA&Ms for 9 of the agency's 22 systems. This is a repeat finding for the third year in a row for three of those systems and for the second year in a row for one system. None of the POA&Ms included separate POA&M items for quarterly system security plan reviews.

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. Three of the identified issues have been corrected; however, the remaining issues below have yet to be addressed:

- 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.
- Does not automatically change the status from on track to delayed once the scheduled completion date has passed.

[5] OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*.

Initial Target Remediation Dates Are Frequently Missed

The agency overall progress in correcting weaknesses reported on its POA&Ms continues to decline. In FY 2012, the agency closed 30 percent of its program level weaknesses and 55 percent of its system level weaknesses, while in FY 2013, the agency closed only 15 percent of its program level weaknesses and 37 percent of its system level weaknesses. In FY 2014, while the agency closed 40 percent of its program level weaknesses, it closed only 27 percent of its system level weaknesses.

Why This Occurred

POA&M Compliance Reviews Are Not Conducted

CSO-PROS-2016 includes a process for conducting independent verification and validation on closed weaknesses and POA&M scoring as part of the CSO IT security continuous monitoring process. POA&M compliance reviews were conducted by the CSO on a quarterly basis; however, they were discontinued at the end of 2012 as the agency began working on updating CSO-PROS-2016, developing a POA&M training program, and defining new scoring metrics. 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 and FY 2014.

Why This Is Important

Progress of Corrective Efforts Cannot Be Effectively Monitored

POA&Ms are intended to track and monitor known information security weaknesses. POA&Ms that do not include all known security weaknesses and are not updated in a timely manner are not effective at monitoring the progress of corrective efforts relative to known weaknesses in IT security controls. As a result, the POA&M does not provide an accurate measure of security program effectiveness.

Recommendation

The issue with the NRC POA&M program is a repeat finding from the FY 2012 and FY 2013 FISMA evaluations. 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.

IV. NEW RECOMMENDATION

OIG recommends that the Executive Director for Operations

1. In support of continuous monitoring, develop a plan and schedule for updating all NRC system security plans, as well as the NRC Information Security Program Plan, to reflect NIST SP 800-53, Revision 4.

V. AGENCY COMMENTS

A discussion draft of this report was provided to the agency prior to an exit conference held on November 13, 2014. At this meeting, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

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

Scope

The evaluation focused on reviewing NRC's implementation of FISMA for FY 2014. 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. Four agency systems were selected for evaluation.

The evaluation was conducted from April 2014 through September 2014. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, evaluators were aware of the possibility of fraud, waste, and abuse in the program.

Methodology

Richard S. Carson & Associates, Inc., conducted an independent evaluation of NRC's implementation of FISMA for FY 2014. 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 2014 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 2014 independent evaluation, including security assessment reports and vulnerability assessment reports prepared in support of system security assessment and authorization.
- Security categorizations, security plans, contingency plans, contingency plan test reports, and ATO memoranda for all agency systems.
- Annual security control assessment reports for all agency systems.

The annual security control assessment report for the agency's common controls was not reviewed, as annual security control testing for these controls had not been completed for FY 2014 by the end of fieldwork.

When reviewing security assessment 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.

- Council of the Inspectors General on Integrity & Efficiency, *Quality Standards for Inspection and Evaluation*, January 2012.

- 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, and Virgil Isola, CISSP, from Richard S. Carson & Associates, Inc.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email:	Online Form
Telephone:	1-800-233-3497
TDD	1-800-270-2787
Address:	U.S. Nuclear Regulatory Commission Office of the Inspector General Hotline Program Mail Stop O5-E13 11555 Rockville Pike Rockville, MD 20852

COMMENTS AND SUGGESTIONS

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

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