OFFICE OF THE INSPECTOR GENERAL

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

Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015

OIG-16-A-03
November 12, 2015

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 12, 2015

MEMORANDUM TO: Victor M. McCree
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 MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2015 (OIG-16-A-03)

Attached is the Office of the Inspector General's (OIG) independent evaluation report titled *Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014* [FISMA 2014] *for Fiscal Year 2015*. The purpose of this evaluation was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2015.

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:

- There is a repeat finding from the FY 2014 FISMA evaluation: 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.
- There is a repeat finding from previous FISMA evaluations: the agency did not provide sufficient documentation to determine if oversight of contractor systems is adequate.

This report presents the results of the subject evaluation. As there were no new findings for FY 2015, this report does not contain additional recommendations to improve the agency's implementation of FISMA 2014. Following the November 9, 2015,

exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

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-16-A-03

November 12, 2015

Results in Brief

Why We Did This Review

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

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

The evaluation objective was to perform an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA 2014 for Fiscal Year 2015.

Independent Evaluation of NRC's Implementation of FISMA 2014 for Fiscal Year 2015

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 repeat findings from previous FISMA evaluations. Specifically, we found that continuous monitoring is not performed as required, configuration management procedures are still not consistently implemented, and plans of action and milestones management still needs improvement. In addition, the agency did not provide sufficient documentation to determine if oversight of contractor systems is adequate.

What We Recommend

There are no new findings for FY 2015. Recommendations for the repeat findings were made in prior reports, and implementation of those recommendations is being tracked through the OIG followup process.

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

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ATO	Authorization to Operate
ATO-CA	Continuous ATO
CP	Contingency Plan
CSO	Computer Security Office
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IT	Information Technology
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
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 18, 2014, the President signed the Federal Information Security Modernization Act of 2014 (FISMA 2014), reforming the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[1] and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor.[2] Office of Management and Budget (OMB) memorandum M-16-03, *Fiscal Year 2015-2015 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2015, requires OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

The U.S. Nuclear Regulatory Commission (NRC) OIG retained Richard S. Carson & Associates, Inc., to perform an independent evaluation of NRC's implementation of FISMA 2014 for fiscal year (FY) 2015. This report presents the results of that independent evaluation. Carson & Associates will also submit responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool in accordance with OMB guidance.

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

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

II. OBJECTIVE

The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2015. Appendix A contains a description of the evaluation objective, scope, and methodology.

III. FINDINGS

NRC has continued to make improvements to its information technology (IT) security program and progress in implementing the recommendations resulting from previous FISMA evaluations. The agency has accomplished the following since the FY 2014 FISMA independent evaluation:

- The agency continued to maintain current authorizations to operate for most agency and contractor systems. In FY 2015, the agency completed security assessments and authorizations of four systems. As of the completion of fieldwork for FY 2015, 17 of the 23 operational information systems had a current authorization to operate (ATO).[3] The agency also completed security assessments for an additional five systems; however, these systems have not yet been issued formal authorizations.[4] All five of these systems are operating without a current ATO as their ATO or ATO extensions have expired. One additional system is also operating without a current ATO as its ATO extension has expired. The agency is in the process of decommissioning this system. A decommission request memorandum has been submitted, but not yet formally

[3] Two operational information systems are operating under an ATO extension. The ATO for one system expired on September 6, 2015, and was extended until December 18, 2015. The ATO for the other system expired on September 28, 2014, and was extended until April 30, 2016. Under certain circumstances, the NRC Designated Approving Authority/Authorizing Official (DAA/AO), who assumes the responsibility for operating an information system at an acceptable level of risk, can grant permission to delay the reauthorization of a system due to the need to continually operate the system in support of the agency's mission. A system owner can request the delay in writing and explain the circumstances (e.g., delays in starting testing, hardware/software upgrades, changes to the system boundary) causing the delay. The DAA/AO responds with a memorandum granting the delay and includes specific conditions that the system owner must meet to minimize the risk of operating the system under the ATO extension.

[4] These systems have been issued a verbal ATO or ATO extension, but no formal memoranda have been issued.

approved. See Appendix B for additional information on systems with an expired ATO or ATO extension.

- The agency updated security plans for 21 operational information systems.

- The agency completed annual security control testing for 11 operational information systems, and security control assessment in support of system authorization for 8 operational information systems.

- The agency completed annual contingency plan testing for 18 operational information systems.

- The agency updated the contingency plans for 15 operational information systems.

- The Computer Security Office (CSO) implemented a Cybersecurity Risk Dashboard to provide high-level view of the agency's security risk by depicting the current risk posture and the status of security risk management activities.

- The CSO issued an Internal Cybersecurity Management Plan in March 2015 that outlines the agency's 5-year cybersecurity program vision and identifies specific efforts targeted to improve the agency's cybersecurity posture, evolve the CSO's operations into a more mature cybersecurity organization, and sets priorities for FY 2015-2020.

- The agency issued several new or updated documents and processes related to IT security including Information Security Program Plan, Information Security Continuous Monitoring Process, System Cybersecurity Coordination Process for New Systems and System Changes, System Cybersecurity Assessment Process, System Artifact Examination Procedure, Plan of Action and Milestones Process, as well as several standards and templates.

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:

- There is a repeat finding from the FY 2014 FISMA evaluation: 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.

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

There are no new findings for FY 2015. Recommendations for the repeat findings were made in prior reports, and implementation of those recommendations 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[5] ATO (ATO-CA), continuous monitoring is essential for determining risk associated with systems and for ensuring risk-based decisions are made concerning continued system operation.

CSO process CSO-PROS-1323, *Information Security Continuous Monitoring Process*, defines the process that must be followed to perform continuous monitoring on systems owned and used by the agency.

[5] NIST uses the term ongoing authorization.

However, some of the required continuous monitoring activities have not been performed. As a result, NRC cannot ensure the effectiveness of information security controls for NRC systems and cannot identify and control risk.

What Is Required

Federal Guidance Regarding Continuous Monitoring

FISMA 2014 requires that agencies establish a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA 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 defines the process that must be followed to perform continuous monitoring on systems owned and used by the agency, and involves five key tasks, as follows:

- Assessing security control effectiveness.
- Addressing risks identified during assessments.
- Maintaining system security documentation.
- Performing required tests.
- Reporting the security state of systems to designated organization officials.

The frequencies for which continuous monitoring activities must be performed are defined in a companion document to CSO-PROS-1323.

Each year, the agency Executive Director for Operations issues a memorandum requiring system owners to perform cybersecurity risk management activities required for FISMA. The purpose of these activities is to identify, control risk, and continuously reduce the cybersecurity operating risk to the NRC mission. All testing activities must be completed and the final test reports dated within the required time frame (e.g., 1 year) of the previous test report date. The agency uses its Cybersecurity Risk Dashboard to specify the status and current due dates of each required activity.

In the FY 2015 memorandum, issued January 2015, system owners were required to take the following actions:

- Perform a Periodic System Cybersecurity Assessment.
- 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, Security Categorization, Privacy Threshold Analysis). System security plans and POA&Ms must be reviewed at least quarterly.

The FY 2015 memorandum also specifically required all system security plans to be updated to reflect NIST SP 800-53 Revision 4 by September 30, 2015.

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.

What We Found

Noncompliance With Continuous Monitoring Guidance

Figure 1 summarizes the required continuous monitoring activities that were not performed by the agency in FY 2015. One of the systems operating under an ATO-CA has not performed any of the required continuous monitoring activities noted below since its ATO-CA was issued in September 2013. One of the systems with an expired ATO for which annual security control testing was not performed is in the process of being decommissioned. However, the last annual security control test for this system was in May 2013, and the request to decommission this system was not made until September 2015.

Figure 1

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

Source: OIG-generated figures from analysis of agency documentation

Some Annual Security Control Assessments Were Delayed

Of the 19 systems that had an annual security control assessment completed in FY 2015, only 5 were not completed within 1 year of the previous year's testing. This is an improvement from FY 2014, when 11 of 16 annual security control assessments were delayed.

Some System Security Plans Were Not Updated Quarterly as Required

Of the 21 system security plans updated in FY 2015, 7 were not updated quarterly as required. Per the FY 2015 risk management activities memorandum, the remaining 14 system security plans should have had an update for the fourth quarter, to be completed by August 15, 2015; however, 9 have not been updated since May 15, 2015.

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. As found in FY 2014, none of the 21 system security plans updated in FY 2015 were updated to include changes to NIST SP 800-53.

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

The issue with continuous monitoring activities, specifically system security plan updates, is a repeat finding from the FY 2014 FISMA evaluation. The recommendation from the FY 2014 FISMA evaluation is 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.

B. NRC Configuration Management Procedures Are Not Consistently Implemented

FISMA 2014 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 2015 FISMA evaluation team found that configuration management procedures are not consistently implemented. Specifically, (i) standard baseline configurations are not implemented on some NRC systems, and (ii) vulnerability remediation and patch management procedures are not consistently implemented. The agency has yet to implement one of the five recommendations from the FY 2011 FISMA evaluation related to configuration management, and two of the five were just completed in July 2015. However, many of the same issues were found again in the FY 2013, FY 2014, and FY 2015 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 2014 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 precedents for the applicability of configuration baselines are 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. Vulnerability scans and configuration checks are one of the five keys tasks for continuous monitoring, as specified in CSO-PROS-1323. Configuration compliance scans, vulnerability scans, and wireless scans are required quarterly and system owners must provide evidence of periodic scanning to the CSO. CSO-PROS-1401, *Periodic System Scanning Process*, describes the process to be used to perform periodic scans on NRC systems.

The cybersecurity risk management activities memorandum and instructions for FY 2015 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 accordance with CSO-PROS-1401.

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

Vulnerability Remediation and Patch Management

CSO standard CSO-STD-0020, *Organization Defined Values for System Security Controls*, 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.

The same timeframes apply to the installation of security-relevant software and firmware updates (e.g., patches, service packs, and hot fixes). The IT cybersecurity risk management activities memorandum and instructions for FY 2015 require system owners to patch, scan, and check the security of their systems with the rigor and frequency appropriate for the system sensitivity level.

What We Found

Noncompliance With Configuration Management Guidance

The FISMA evaluation team reviewed the security control assessment results for the 19 operational information systems for which some type of

security control assessment was performed in FY 2015 – 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 2015 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 18 of the 19 systems tested in FY 2015. 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.

Vulnerability Remediation and Patch Management Procedures Are Not Consistently Implemented

As reported in previous FISMA evaluations, the FY 2015 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 11 of the 19 systems tested in FY 2015 continue to have issues remediating the vulnerabilities in a timely manner.

Why This Occurred

Corrective Actions From Previous FISMA Evaluations Have Not Been Completed

The agency has yet to implement one of the five recommendations from the FY 2011 FISMA evaluation related to configuration management, and two of the five were just completed in July 2015. However, many of the

same issues were found again in the FY 2013, FY 2014, and FY 2015 evaluations.

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, FY 2013, and FY 2014 FISMA evaluations. One of the five recommendations from the FY 2011 FISMA evaluation is 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 2014, 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 identifying and tracking the status of security weaknesses for a system. 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 2015 FISMA evaluation team found that NRC's POA&M process was not consistently followed. 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, FY 2014, and FY 2015. 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 2014 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.

Internal POA&M Guidance

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

- POA&Ms must be updated to add weaknesses identified in formal documentation resulting from a variety of cybersecurity activities

including, but not limited to security control assessments, vulnerability scans, configuration compliance checks, contingency plan testing, 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 21 calendar days from the final publication date of the document or report that identifies the weakness.

- POA&Ms should be reviewed and maintained on an ongoing basis, at least monthly, to ensure the POA&M accurately reflects the current status of tracked POA&M items.

The IT cybersecurity risk management activities memorandum and instructions for FY 2015 require all updates to be entered into the automated tool before the quarterly snapshot updates (the 15th of November, February, May, and August).

CSO procedure CSO-PROC-2104, *System Artifact Examination Procedure*, specifies the procedures used to evaluate cybersecurity artifacts for acceptability, including acceptability criteria for POA&Ms. A POA&M is considered to be deficient if one or more of eight criteria are found, including the following:

- POA&M exists but four or more of the open POA&M items have completion due dates that are more than 1 year old; or
- POA&M exists but greater than 25 percent of the open POA&M items have completion due dates that are more than 1 year old.

In April 2015, the agency issued a memorandum authorizing the discontinuation of tracking low cybersecurity risks as POA&M items. The agency's rationale for this decision is that most low risks identified during assessments are items that should be addressed during regular system maintenance. CSO-PROS-2016 adds that if low severity items are not addressed during normal system maintenance, then their severity may be elevated and POA&M creation required.

What We Found

Noncompliance With POA&M Guidance

As the agency has yet to complete the two recommendations from the FY 2012 FISMA evaluation related to the POA&M process, instead of reviewing all of the FY 2015 POA&Ms to determine whether the agency is following POA&M guidance, the FY 2015 evaluation team (1) reviewed a sampling of FY 2015 POA&Ms and (2) also reviewed the security control assessment results for the 19 operational information systems for which some type of security control assessment was performed in FY 2015 – specifically test results or assessor concerns related to control CA-5, POA&Ms.

The FY 2015 FISMA evaluation team also applied the agency's own criteria from CSO-PROC-2104 to determine whether the FY 2015 Q4 POA&Ms are acceptable cybersecurity artifacts.

POA&Ms Do Not Include All Known Security Weaknesses

As reported in several previous FISMA evaluations, the FY 2015 FISMA evaluation team found some IT-related weaknesses were not added to the POA&Ms as required by agency policy.

- The recommendation from the FY 2014 FISMA independent evaluation has not been added to the appropriate POA&M.
- Weakness identified by periodic scanning were not added to one system's POA&M.

POA&Ms Are Not Updated in a Timely Manner

As reported in several previous FISMA evaluations, the FY 2015 FISMA evaluation team found POA&Ms are not updated in a timely manner. The following are some examples of updates that are not timely.

- Weaknesses closed by OIG are still not being reported as closed on the POA&Ms.

- The program level POA&M and multiple system POA&Ms continue to include large numbers of weaknesses that are more than 1 year old. One system POA&M has more than 150 weaknesses that are more than 1 year old and should no longer be reported. OMB guidance[6] 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.

Initial Target Remediation Dates Are Frequently Missed

FY 2015 security control assessment reports for three systems reported delayed POA&Ms as a significant concern.

The security control assessment for one system found that low risk weaknesses were not being addressed as part of normal system maintenance. Therefore, the ATO recommendation included a system specific condition to move all low risk weaknesses to moderate.

POA&Ms Do Not Meet NRC Acceptability Criteria

The FY 2015 evaluation team found that 13 of the 23 FY 2015 Q4 systems POA&Ms, as well as the agency's program level POA&M, do not meet NRC acceptability criteria for cybersecurity artifacts and are considered deficient.

Why This Occurred

POA&M Compliance Reviews Are Not Conducted

CSO-PROS-2016 includes a process for the CSO Policy, Compliance, and Training Senior IT Security Officer to review and approve closed weaknesses and for the CSO to conduct quarterly POA&M reviews to ensure they are being maintained as required. The new processes were not effective until October 1, 2015, and the agency has yet to complete the two recommendations from the FY 2012 FISMA evaluation related to the

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

POA&M process; therefore, many of the same issues were found again in FY 2013, FY 2014, and FY 2015.

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, FY 2013, and FY 2014 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.

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

FISMA 2014 requires agencies to ensure the adequate protection of agency information, including information collected or maintained by contractors, as well as information systems operated by contractors on the agencies' behalf. NRC has policies for performing oversight of contractor systems. However, NRC did not provide a current system inventory of contractor systems and did not provide requested documentation to demonstrate oversight of contractor systems is performed. In addition, two corrective actions from the FY 2013 FISMA evaluation related to oversight of contractor systems were reported completed by the agency in September 2015; however, the agency did not provide sufficient evidence that one of the recommendations was actually completed. As a result, the FY 2015 evaluation team was unable to determine if oversight of contractor systems is adequate.

What Is Required

Federal Requirements for Oversight of Contractor Systems

FISMA 2014, Section 3554(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3554(b) requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." This includes services that are provided (in full or in part) by another Federal agency, outsourced to a commercial vendor, and cloud solutions such as software-as-a-service.

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed for all contractor systems. Agencies must ensure identical, not "equivalent," security procedures. For example, annual testing and evaluation, risk assessments, security plans, security control assessments, contingency planning, and security authorization must also be performed for all contractor systems.

Internal Guidance Regarding Oversight of Contractor Systems

Management Directive and Handbook 12.5, *NRC Cyber Security Program*, require Federal agencies or third-party service providers hosting NRC capabilities to meet NRC cyber security requirements. CSO-PROS-2030 describes the process for applying the RMF described in NIST SP 800-37, Revision 1, to secure NRC systems, including contractor systems.

CSO-PROS-1323 defines the process that must be followed to perform continuous monitoring on systems owned and used by the agency, including systems owned and/or operated by other agencies.

Each year, the agency Executive Director for Operations issues a memorandum requiring system owners to perform cybersecurity risk management activities required for FISMA, including annual requirements

for systems authorized by other agencies. For such systems, the applicable NRC Office Director must perform several actions, including, but not limited to the following:

- Verify that day-to-day security operations of the interconnected system(s) are carried out including periodic vulnerability assessment scanning, annual CP testing and periodic control testing.

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

- Ensure that the sponsoring agency maintains the system ATO in accordance with NIST SP 800-37 and provide the most recent sponsoring agency-issued ATO memorandum to CSO, ensuring that only fully authorized systems are used by or on behalf of NRC.

What We Found

Insufficient Documentation Provided

NRC did not provide a current system inventory of contractor systems and did not provide requested documentation to demonstrate oversight of contractor systems is performed. In addition, two corrective actions from the FY 2013 FISMA evaluation related to oversight of contractor systems were reported completed by the agency in September 2015; however, the agency did not provide sufficient evidence that one of the recommendations was actually completed.

Why This Is Important

Adequacy of Oversight of Contractor Systems Could Not Be Determined

Without a current system inventory of contractor systems or documentation required by the NRC continuous monitoring program for

systems authorized by other agencies, the FY 2015 evaluation team was unable to determine if oversight of contractor systems is adequate.

Recommendation

The issue with oversight of contractor systems is a repeat finding from the FY 2013 FISMA evaluation. One of the three recommendations from the FY 2013 FISMA evaluation is 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. CONSOLIDATED LIST OF RECOMMENDATIONS

All of the findings are repeat findings. Therefore, OIG is not issuing any new recommendations for FY 2015.

V. AGENCY COMMENTS

A discussion draft of this report was provided to the agency prior to an exit conference held on November 9, 2015. At this meeting, agency management stated their general agreement with the findings in this report and opted not to provide formal comments for inclusion in this report.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2015.

Scope

The evaluation focused on reviewing NRC's implementation of FISMA 2014 for FY 2015. The evaluation included an assessment of the effectiveness of the NRC's information security policies, procedures, and practices, and a review of information security policies, procedures, and practices of a representative subset of 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 2015 through September 2015. 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 2014 for FY 2015. In addition to an assessment of the effectiveness of the NRC's information security policies, procedures, and practices, the evaluation included an assessment of the following topics specified in OMB's FY 2015 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.

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

- NRC policies, procedures, and guidance specific to NRC's IT security program and its implementation of FISMA 2014, and to the 10 topics specified in OMB's reporting metrics.
- Security assessment and authorization documents for the four systems selected for evaluation during the FY 2015 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 agency systems.
- Annual security control assessment reports for agency systems.

When reviewing security assessment reports, the team focused on security controls specific to the 10 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 guidance.

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

Appendix B

SYSTEMS WITH AN EXPIRED ATO OR ATO EXTENSION

The following table provides additional details on operational systems operating with an expired ATO or ATO Extension.

System	ATO Expiration	ATO Extension Expiration	Comments
System 1	01/20/14	09/30/15	Verbal ATO granted 09/29/15
System 2	01/20/14	06/30/15	Verbal Extension through 08/31/15 granted on 06/09/15 Verbal ATO granted 07/31/15
System 3	11/09/14	09/30/15	Decommission request submitted 09/28/15
System 4	09/06/15	N/A	Verbal Extension through 12/31/15 granted on 06/09/15
System 5	11/16/14	09/30/15	Verbal Extension through 12/31/15 granted on 09/29/15
System 6	07/26/13	08/24/14	Verbal ATO granted 07/31/15

Source: OIG created from analysis of agency documentation

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.