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

OFFICE OF THE
INSPECTOR GENERAL

December 21, 2017

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: SUMMARY REPORT OF FISMA EVALUATIONS CONDUCTED IN FISCAL YEAR 2017 (OIG-18-A-08)

The Office of the Inspector General (OIG) is issuing this memorandum report to summarize the findings and recommendations of the six *Federal Information Security Modernization Act of 2014* (FISMA) evaluations conducted in Fiscal Year (FY) 2017. FISMA outlines the information security management requirements for Federal agencies, which includes an independent evaluation of the agency's information security program and practices to determine their effectiveness.

Each regional office and the Technical Training Center (TTC) is responsible for implementing the Nuclear Regulatory Commission's (NRC) information security program at their location. In order to evaluate the effectiveness of NRC's information security program and practices across the entire agency, NRC OIG conducts periodic independent evaluations at the regional offices and TTC.

Overall, the six FY 2017 FISMA evaluations at Headquarters (HQ), the Regions, and TTC resulted in 9 findings and 14 recommendations to address those findings. There was one management issue identified, but there were no recommendations made. As such, there are no new recommendations in this summary report.

BACKGROUND

On December 18, 2014, the President signed into law FISMA, which outlines the information security management requirements for agencies, which includes an annual independent evaluation of an agency's information security program and practices to determine their effectiveness.

FISMA requires the annual evaluation to be performed by the agency's OIG or by an independent external auditor. NRC OIG retained Richard S. Carson & Associates, Inc., to perform an independent evaluation of NRC's implementation of FISMA for FY 2017, which, in addition to the evaluation conducted at NRC HQ, included a separate evaluation of NRC's four regional offices and TTC.

NRC has four regional offices that conduct inspection, enforcement, investigation, licensing, and emergency response activities for nuclear reactors, fuel facilities, and materials licensees. Additionally, NRC's TTC, located in Chattanooga, Tennessee, provides training for staff in various technical disciplines associated with the regulation of nuclear materials and facilities. Each regional office and the TTC is responsible for implementing the NRC's information security program at their location.

OBJECTIVE

The objective of this report is to summarize the findings and recommendations of the six FISMA evaluations conducted in FY 2017.

SYNOPSIS OF EACH REPORT

Headquarters FISMA Evaluation

The NRC HQ FISMA evaluation work was conducted from June to September 2017, and had two findings related to Information Technology (IT) security program documentation and continuous monitoring activities. The IT security program documentation, including policies, process, procedures, guidance, standards, and templates are not up-to-date. This is due to responsibilities for the IT security program documentation maintenance changing. Also, IT security program documentation maintenance is not current, and it has not been a priority. The second finding concluded that some security categorizations, contingency plans, and business impact assessments are not updated annually as required because (1) their status is not visible in the Cybersecurity Risk Dashboard, (2) the security categorization procedures are in the process of being updated, and (3) procedures for monitoring completion of all continuous monitoring activities are lacking. This evaluation resulted in the OIG making a combined seven recommendations for the two findings.

The full report is available at https://www.nrc.gov/docs/ML1730/ML17303A870.pdf.

Region I FISMA Evaluation

The Region I FISMA evaluation work was conducted from May 22, 2017 to May 26, 2017, and had one finding. High risk and moderate risk findings were identified in components when a network vulnerability scan of the

Region I network, including its Incident Response Center network, and the Region I Resident Inspector sites was performed. Region I had not been including components of the Region I incident response center in its vulnerability scans because the equipment is proprietary, and there was a concern that network scans might cause the equipment to go off-line. OIG made one recommendation to address this finding.

The full report is available at https://www.nrc.gov/docs/ML1718/ML17184A010.pdf.

Region II FISMA Evaluation

The Region II FISMA evaluation work was conducted from March 27, 2017 to March 31, 2017, and had one finding. Backups were not being performed at the Region because Region II did not attempt to repair the failed local backup server after it began experiencing hardware failures in January 2017. At the time of the evaluation, Region II was in the process of replacing all of the Windows 2003 servers with Windows 2012 servers. Region II determined that efforts to support the deployment of the new Windows 2012 servers took precedence over repairing or replacing the backup server. OIG made no recommendations for this finding because the target deployment date for the new servers was the end of April 2017.

The full report is available at https://www.nrc.gov/docs/ML1712/ML17122A113.pdf.

Region III FISMA Evaluation

The Region III FISMA evaluation work was conducted from April 24, 2017 to April 28, 2017, and had no findings, but identified a management issue. During the evaluation, division instructions were reviewed and revised within the past year, and the hyperlink of the final approved procedure or instruction in the NRC Agencywide Document Access and Management System (ADAMS) was emailed to all Region III employees. However, the links to the documents on the Region III Web site did not point to the current final approved versions in ADAMS. Because there were no findings, OIG did not make any recommendations for the Region III office, but noted that employees might not be able to find the current versions of these documents on the Region III internal Web site.

The full report is available at
https://www.nrc.gov/docs/ML1715/ML17151A244.pdf.

Region IV FISMA Evaluation

The Region IV FISMA evaluation work was conducted from July 17, 2017 to July 21, 2017 and had three findings related to Region IV's policy guides, backup documentation, and network vulnerabilities. Some Region IV policy guides have not been reviewed and updated as required. Region IV's backup documentation has not been reviewed and does not describe backup procedures for the IT support server, including procedures for sending backup tapes to an offsite storage location. Also, high risk and moderate risk findings were identified during a vulnerability scan of the Region IV network, the Region IV Resident Inspector sites, and some components that support alternate processing capabilities for NRC Headquarters. OIG made one recommendation per finding for Region IV.

The full report is available at
https://www.nrc.gov/docs/ML1726/ML17263A196.pdf.

TTC FISMA Evaluation

The TTC FISMA evaluation work was conducted from June 19, 2017 to June 23, 2017 and had two findings related to inventory and managing Authorizations to Operate (ATO). The TTC hardware and software inventory has not been updated to include new components that were part of a simulator upgrade project. The simulator network components were never physically assessed, so they were not added to the TTC Hardware and Software Inventory document. Also, the TTC had a laptop with a lapsed ATO. Additionally, there were approximately 80 other laptops and standalone desktops that were not part of the TTC system boundary, have not had any type of system cybersecurity assessment, and were not formally authorized to operate. As a result of this evaluation, OIG made three recommendations to address the two findings.

The full report is available at
https://www.nrc.gov/docs/ML1722/ML17229B479.pdf.

FINDINGS AND RECOMMENDATIONS

Overall, the FY 2017 FISMA evaluations at Headquarters, the Regions, and the TTC resulted in 9 findings and 14 recommendations to address those findings. There was one management issue that did not result in any findings or recommendations.

Table 1: Breakdown of Findings and Recommendations

Number of Findings	Topic	Recommendations
3	IT documentation was not up-to-date.	3 (HQ) 2 (Region IV)
2	Vulnerability scans identified high risk and moderate risk findings.	1 (Region I) 1 (Region IV)
1	Continuous monitoring activities were not performed as required.	4 (HQ)
1	Backups were not being performed on the local backup server.	0 (Region II)
1	Inventory was not updated to reflect new components.	1 (TTC)
1	One laptop with a lapsed ATO and approximately 80 other laptops and standalone desktops were never issued an ATO.	2 (TTC)

Source: OIG Analysis of FISMA Reports Conducted in FY 2017.

Management Issue	Topic	Recommendations
1	Links on the internal Web site do not lead to the most current division instructions that have final approval in ADAMS.	0 (Region III)

Source: OIG Analysis of FISMA Reports Conducted in FY 2017.

SUMMARY AND CONCLUSION

In summary, the FY 2017 FISMA evaluations resulted in 9 findings and 14 recommendations to address those findings. Three findings concerned IT documentation not being up-to-date. Specifically, at HQ, IT security program documentation is not up-to-date. In Region IV, policy guides and backup documentation have not been reviewed and updated as required. Two similar findings were documented in two of the Regions (Regions I and IV) because vulnerability scans identified high risk and moderate risk findings. Four findings were unique to their Regions. The findings addressed not performing continuous monitoring activities; backups not being performed on the local backup server; inventory not being updated; and authorizations to operate laptops and standalone desktops not being kept up-to-date or issued at all.

The evaluations did not identify any major IT security weaknesses. Additionally, NRC has made significant improvements in the effectiveness of its IT security program, and continues to make improvements in performing continuous monitoring activities.

While multiple findings were identified, no single finding extended across all six evaluations conducted. The most prevalent issue identified was IT documentation not being up-to-date. Specifically, three recommendations were made to HQ to address this issue and two recommendations were made to Region IV. There are no new findings or recommendations in this summary report.

AGENCY COMMENTS

On November 21, 2017 a discussion draft was provided to the agency for their comment. After review of the discussion draft, agency management opted not to provide formal comments for inclusion in this report.

SCOPE AND METHODOLOGY

Scope

The scope of this summary report is a review and summary of the six FISMA evaluations conducted during FY 2017. This work was conducted at NRC Headquarters in Rockville, Maryland from November 3, 2017 to November 20, 2017.

Methodology

We analyzed all six FISMA evaluation reports conducted during FY 2017, to identify repeat findings and recommendations. The findings and recommendations from the six evaluations are summarized in Table 1 of this report.

All analyses were performed in accordance with Council of the Inspectors General on Integrity & Efficiency, *Quality Standards for Inspection and Evaluation*, January 2012.

The following are criteria for evaluating IT security at NRC

- The National Institute of Standards and Technology standards and guidelines.
- Management Directive and Handbook 12.5, *NRC Cybersecurity Program*.
- NRC Information Security Planning and Oversight Branch policies, processes, procedures, standards, and guidelines.

This summary report was prepared by Beth Serepca, Team Leader; Kristen Lipuma, Audit Manager, and Janelle Wiggs, Auditor.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email:	Online Form
Telephone:	1-800-233-3497
TDD	7-1-1, or 1-800-201-7165
Address:	U.S. Nuclear Regulatory Commission Office of the Inspector General Hotline Program Mail Stop O5-E13 11555 Rockville Pike Rockville, MD 20852

COMMENTS AND SUGGESTIONS

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

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