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

OFFICE OF THE
INSPECTOR GENERAL

July 3, 2017

MEMORANDUM TO:	Victor M. McCree Executive Director for Operations
FROM:	Dr. Brett M. Baker ***/RA/*** Assistant Inspector General for Audits
SUBJECT:	INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FY 2017 REGION I, KING OF PRUSSIA, PA (OIG-17-A-17)

The Office of the Inspector General (OIG) conducted an independent evaluation of NRC's implementation of FISMA 2014 for Fiscal Year (FY) 2017 at the Region I office located in King of Prussia, PA. The OIG found that the Region I information technology (IT) security program, including Region I IT security policies, procedures, and practices, is generally effective. However, a network vulnerability scan found vulnerabilities and OIG recommends that these vulnerabilities be remediated within the required timeframes. 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.

BACKGROUND

The U.S. Nuclear Regulatory Commission (NRC) has four regional offices that conduct inspection, enforcement, investigation, licensing, and emergency response programs for nuclear reactors, fuel facilities, and materials licensees. The Region I office oversees regulatory activities in the northeastern United States; is located in King of Prussia, PA; and operates under the direction of a Regional Administrator.

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 or by an independent external auditor.[2]

The NRC OIG retained Richard S. Carson & Associates, Inc., to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017 at NRC's four regional offices and the Technical Training Center (TTC). This report presents the results of the independent evaluation at the NRC's Region I office.

[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 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…."

OBJECTIVE

The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017 at NRC's Region I office and to evaluate the effectiveness of agency information security policies, procedures, and practices as implemented in this location.

RESULTS

The Region I IT security program, including Region I IT security policies, procedures, and practices, is generally effective. However, a network vulnerability scan found vulnerabilities that require remediation.

Network Vulnerability Scan Found Vulnerabilities That Require Remediation

Federal guidance requires agencies to scan for vulnerabilities in information systems and remediate legitimate vulnerabilities within organization-defined response times. NRC has developed processes for performing periodic scans and for remediating vulnerabilities identified by scans. A network vulnerability scan of the Region I network, including its Incident Response Center (IRC) network, and the Region I Resident Inspector sites, found vulnerabilities that require remediation. Vulnerabilities were found in IT components owned by Region I and NRC IT Infrastructure (ITI) components.[3] Vulnerabilities in these components could result in disclosure of, or unauthorized access to, sensitive information, unauthorized privileged access, deletion of data, uploading unauthorized content, and denial of service.

[3] Region I IT components are managed by Region I staff. ITI components are managed by the NRC's seat-management contractor.

What Is Required

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to scan for vulnerabilities in information systems and remediate legitimate vulnerabilities within organization-defined response times. Information Security Directorate (ISD) process ISD-PROS-2030, *NRC Risk Management Framework (RMF) 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 ISD-PROS-1323, *Information Security Continuous Monitoring Process*.

ISD standard ISD-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.

ISD Process ISD-PROS-1324, *Deviation Request Process*, describes the process for NRC to identify security weaknesses that qualify for deviation requests and the process of submitting a deviation request. For example, it may be either not technically feasible or too costly to remediate a weakness identified by a vulnerability scan, or the required corrective action could have an unwanted impact on normal business processes. Deviation requests are submitted by the system owner and reviewed and approved, or denied by the designated approving authority.

What We Found

The evaluation team performed a network vulnerability assessment scan of the Region I network, including its IRC network, and the Region I Resident Inspector sites. All scan targets were physically located in Region I and included IT components owned by Region I, as well as components owned by the NRC IT Infrastructure (ITI). Specifically, high risk and moderate risk findings were identified in components.

Why This Occurred

The majority of the vulnerabilities were identified in equipment in the Region I IRC. This equipment is proprietary and Region I had not been including those components in periodic vulnerability scanning activities due to concerns the scans might cause the equipment to go off-line. All but one of the remaining vulnerabilities were identified in ITI equipment that is managed by NRC's seat-management contractor.

Why This Is Important

The equipment must be available at all times as it supports emergency operations functions. Vulnerabilities in this equipment could result in disclosure of or unauthorized access to sensitive information, unauthorized privileged access, deletion of data, uploading unauthorized content, and denial of service. The Region I component provides Web services, and vulnerabilities in this component could result in unauthorized access to sensitive information. The ITI components provide security services, file services, and network services. Vulnerabilities in ITI components could also result in disclosure of sensitive information, unauthorized privileged access, and denial of service.

RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Remediate the identified vulnerabilities within the timeframes specified in ISD standard ISD-STD-0020, *Organization Defined Values for System Security Controls*, or submit a deviation request in accordance with ISD Process ISD-PROS-1324, *Deviation Request Process*.

AGENCY COMMENTS

An exit conference was held with the agency on May 26, 2017. After this meeting, a discussion draft was provided to the agency for their comment. Agency management stated their general agreement with the results and opted not to provide formal comments for inclusion in this report.

SCOPE AND METHODOLOGY

Scope

The scope of this evaluation included

- The three floors Region I occupies at 2100 Renaissance Boulevard, Suite 100, King of Prussia, PA 19406-2713.
- Region I seat-managed IT components and NRC-managed IT components.
- National security systems (including systems processing safeguards information) housed at Region I.

The evaluation work was conducted during a site visit to Region I in King of Prussia, PA, between May 22, 2017, and May 26, 2017. Any information received from NRC 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 considered the possibility of fraud, waste, or abuse in the program.

Methodology

The evaluation assessed the following focus areas: inventory of systems, the NRC Risk Management Framework and Authorization Process for systems, logical access controls and privileged access, contingency planning, configuration management, and IT security architecture. The evaluation team conducted site surveys of two rooms housing national security systems (including systems processing safeguards information) and the Region I IRC.

The team reviewed documentation provided by Region I including floor plans; inventories of IT systems, hardware, and software; local policies and procedures; security plans; operations guides and standard operating procedures; contingency plans and business impact assessments; configuration management plans; and the Occupancy Emergency Plan. The team conducted interviews with the Region I Information Systems Security Officer (ISSO), deputy ISSO, server administrators, and other Region I employees responsible for implementing the

NRC IT security program at Region I. The evaluation team also conducted user interviews with 15 Region I employees, including 1 Resident Inspector, and 1 teleworker.

The information security risk evaluation also included a network vulnerability assessment scan of the Region I network, including its IRC network, and the Region I Resident Inspector sites. The evaluation team immediately notified Region I of any critical vulnerabilities that were found. Subsequent to the completion of fieldwork, Region I was provided with full details on all of the vulnerabilities identified by the scan.

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 Cybersecurity Program*.
- NRC Information Security Directorate policies, processes, procedures, standards, and guidelines.
- NRC OIG guidance.

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

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.