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

OFFICE OF THE
INSPECTOR GENERAL

May 31, 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 FISCAL YEAR 2017 – REGION III, LISLE, IL (OIG-17-A-15)

The Office of the Inspector General (OIG) conducted an independent evaluation of NRC's implementation of FISMA 2014 for Fiscal Year 2017 at the Region III office located in Lisle, Illinois. OIG found that the Region III information technology (IT) security program, including Region III IT security policies, procedures, and practices, is generally effective. Although OIG makes no recommendations, an opportunity for improvement exists in regard to disseminating Region III procedures, notices, and divisional instructions.

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 regional offices are the agency's front line in carrying out its mission and implementing established agency policies and programs nationwide. The Region III office oversees regulatory activities in the northern midwestern United States; is located in Lisle, Illinois; 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]

[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…."

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

OBJECTIVE

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

RESULTS

The Region III IT security program, including Region III IT security policies, procedures, and practices, is generally effective. Although OIG makes no recommendations, an opportunity for improvement exists in regard to disseminating Region III procedures, notices, and divisional instructions.

Region III uses regional procedures, regional notices, and division instructions to inform the employees of standardized regional practices, division-level directives related to policy and operational matters, and general information. These include policies, procedures, and practices specific to the Region III IT security program. Regional Procedure (RP) 3.57, *System of Procedures, Notices, and Division Instructions* (RP-3.57), describes activities associated with the development, revision, and cancellation of regional procedures, regional notices, and division instructions, and specifies the frequency of review/revision.

RP-3.57 requires the Records Manager to maintain a procedures and divisional instructions (P&DI) index database, which is available on the Region III internal Web page. In addition, as part of the approval and distribution process, within 2 business days of final approval, a hyperlink to the final approved procedure or instruction in the NRC Agencywide Document Access and Management System (ADAMS) is emailed to all Region III employees. The Region III internal Web site also includes links to regional procedures, regional notices, and division instructions.

The evaluation team examined the following divisional instructions and confirmed that they were all reviewed and revised within the past year and that the final approved versions are located in ADAMS.

- DI-12.1, Badging Procedures
- DI-12.1.1, Region III Security System Testing Process
- DI-NR-008, Server Administration
- DI-NR-009, PBX Administration

However, links to the documents on the Region III internal Web site did not point to the current final approved versions in ADAMS, but rather to copies of previous versions stored locally on the Region III Web site. In some cases, the P&DI index had also not been revised to reflect the correct approved date. As a result, employees might not be able to find the current versions of these documents on the Region III internal Web site.

MANAGEMENT ISSUE

In order to improve methods for disseminating Region III procedures, notices, and divisional instructions, Region III should update RP-3.57 to include procedures for maintaining links on the Region III Web site as part of the notification process, and to specify a timeframe for revising the P&DI index after a regional procedure, regional notice, or division instruction has been reviewed/revised. Region III should also consider changing the links on the Region III Web site to point to the final approved versions of the documents in ADAMS rather than to copies stored locally on the Region III Web site.

AGENCY COMMENTS

An exit conference was held with the agency on April 28, 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 III occupies at 2443 Warrenville Road, Suite 210, Lisle, Illinois 60532-4352.
- Region III seat-managed IT components and NRC-managed IT components.
- National security systems (including systems processing safeguards information) housed at Region III.

The evaluation work was conducted during a site visit to Region III in Lisle, IL, between April 24, 2017, and April 28, 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).

The team reviewed documentation provided by Region III 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 III Information Systems Security Officer, server administrators, and other Region III employees

responsible for implementing the NRC IT security program at Region III. The evaluation team also conducted user interviews with 15 Region III employees, including one Resident Inspector, one Resident Inspector administrative assistant, and one teleworker.

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.