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

OFFICE OF THE
INSPECTOR GENERAL

September 20, 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 IV, ARLINGTON, TEXAS (OIG-17-A-25)

The Office of the Inspector General (OIG) conducted an independent evaluation of NRC's implementation of the *Federal Information Security Modernization Act of 2014* (FISMA 2014) *for Fiscal Year (FY) 2017* at Region IV, located in Arlington, Texas. OIG found the Region IV IT security program, including Region IV IT security policies, procedures, and practices, is generally effective. However, some regional policy guides are not up-to-date; Region IV backup procedures are incomplete and not up-to-date; and a network vulnerability scan found vulnerabilities that require remediation. Therefore, OIG makes three recommendations. Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this report. Actions taken or planned are subject to OIG followup as stated in Management Directives 6.1.

BACKGROUND

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 IV office oversees regulatory activities in the western and southern midwestern United States; is located in Arlington, TX; and operates under the direction of a Regional Administrator.

On December 18, 2014, the President signed 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]

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. This report presents the results of the independent evaluation at the NRC's Region IV 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 IV office and to evaluate the effectiveness of agency information security policies, procedures, and practices as implemented in this location.

RESULTS

The Region IV Information Technology (IT) security program, including Region IV IT security policies, procedures, and practices, is generally effective. However, some regional policy guides are not up-to-date; Region IV backup procedures are incomplete and not up-to-date; and a network vulnerability scan found vulnerabilities that require remediation.

Some Regional Policy Guides Are Not Up-to-Date

Region IV uses regional office policy guides and notices to inform the employees of regional policies, procedures, and guidance, including those specific to the Region IV IT security program. Consistent with agency guidance, regional guidance requires policy guides be updated within 3 years of the date of issuance to ensure all information remains correct. Some policy guides require annual review. The evaluation team examined Region IV policy guides and found that some have not been reviewed and updated as required. As a result, important steps or processes could be missed. In addition, outdated procedures make it more difficult when training new personnel to handle a specific activity.

What Is Required

Region IV uses regional office policy guides and notices to inform the employees of regional policies, procedures, and guidance, including those specific to the Region IV IT security program. Policy Guide (PG) 0001.13, *RIV Policy Guide and Office Notice System*, describes activities associated with initiating, revising, and deleting regional policy guides and notices. Policy guides must be updated within 3 years of the date of issuance to ensure all information remains correct. PG 0001.13 also specifies four policy guides that require annual review.

What We Found

Region IV has over 110 published policy guides. The evaluation team examined six of the policy guides related to IT security that require 3 year review/update, and all of the policy guides that require annual review. The following Region IV policy guides have not been reviewed and updated in accordance with PG 0001.13.

Policy guides requiring 3 year review/update:

- PG 0001.13, *RIV Policy Guide & Office Notice System*, issued August 23, 2013.
- PG 0107.4, *Control and Use of COMSEC Devices in Region IV*, issued September 11, 2008.
- PG 0253.5, *Computer User's Guide*, issued April 19, 2012.
- PG 0754.3, *Physical Security Plan Staff Implementing Procedures*, issued September 5, 2013.

Policy guides requiring 1 year review/update:[3]

- PG 0109.3, *Reimbursement for Planned Agency Use of Personal Cellular Telephones*, issued May 29, 2014.
- PG 0453.4, *Potassium Iodide Usage and Guidance*, issued September 5, 2013.
- PG 0759.4, *Region IV Security Program*, issued May 2, 2013.

[3] One of the four policy guides requiring annual review, PG 9015C, *Oversight Process for DRP Metrics*, has been deleted (retired).

Why This Is Important

Outdated procedures can result in important steps or processes being missed. In addition, outdated procedures make it more difficult when training new personnel to handle a specific activity. Current procedures ensure continuity in performing a specific IT security function in the event of staff turnover, are useful for training new personnel and serve as reference for existing personnel.

RECOMMENDATION

OIG recommends that the Executive Director for Operations

1. Update Region IV policy guides that are due for review in accordance with PG 0001.13.

Region IV Backup Procedures Are Incomplete and Not Up-to-Date

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and NRC standards detail requirements for backups of IT systems. Backups are an important part of contingency planning and are a means to restore system operations quickly and effectively following a service disruption. However, Region IV backup procedures are incomplete and not up-to-date. Incomplete and outdated procedures can result in important steps or processes being missed.

What Is Required

NIST SP 800-53, Revision 4, requires organizations to conduct backups of user-level and system-level information, as well as information system documentation, at a frequency defined by the organization consistent with recovery time and recovery point objectives.

Information Security Directorate (ISD) standard ISD-STD 2002, *System Back-up Standard*, states backup and recovery procedures are to be developed, documented, approved, maintained, and used for all systems operated by or on behalf of NRC.

NRC ISD standard ISD-STD-2001, *Operating Procedures Standard*, states that documented and periodically reviewed operational procedures and responsibilities capture the requirements for secure operation of information systems and effective management and support of IT systems. This standard requires system owners to ensure operating procedures are reviewed and approved on a periodic basis, at least annually.

What We Found

Region IV is supported by IT components that are seat-managed (managed by NRC's seat-management contractor) and that are NRC-managed (managed by NRC staff). Seat-managed components provide core IT services at Region IV, and include security appliances, routers, switches, servers (e.g., domain controllers, mail servers, file servers, multi-purpose servers, print servers), desktops, laptops, and printers. NRC's seat-management contractor is responsible for backups of seat-managed servers. These backups occur over the network and are performed by seat-management contractors at NRC headquarters.

Additional IT components located in Region IV are owned and managed by Region IV and include an application server, a Web server, and an IT support file server. Region IV is responsible for backups of these servers. Backups of the application server and Web server are written to external hard drives and include full backups, differential backups, and full image backups. The external drives are stored in a safe when not in rotation. Backups of the IT support server are written to a local tape server. Tapes are stored in a safe when not in rotation and tapes are also sent to offsite storage once a week.

Region IV developed a document, dated February 2015, that describes procedures for performing backups of the application server and Web server. The document includes information on backup types and frequencies, retention period and storage, use of the backup software, backup validation and logs, and recovery testing. However, this document does not describe backup procedures for the IT support server, including procedures for sending backup tapes to an offsite storage location. In addition, this document is an operating procedure and thus subject to the ISD STD 2001 annual review requirement.

Why This Is Important

Backups ensure information necessary for operations is available for restoring system and mission supported operations. System backups ensure critical information integrity and availability in the event of data corruption, hardware failure, or sitewide disaster. Backups need to be sent to an offsite storage location to allow for recovery from situations in which the primary facility is damaged or inaccessible. While software performs many of the backups automatically, someone must ensure the backup jobs include all required servers and run without errors. Incomplete and outdated procedures can result in important steps or processes being missed. The procedures need to be documented and current so that if the primary personnel responsible for server administration are not available, alternates have the information necessary to follow the procedures. Current procedures can also be useful when training new employees with responsibilities for server administration.

RECOMMENDATION

OIG recommends that the Executive Director for Operations

2. Update the backup procedures for Region IV NRC-managed servers to include backup procedures for the Region IV IT support server and for sending backups to an offsite storage location.

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 IV network, including its Incident Response Center (IRC) network, the Region IV Resident Inspector sites, and some components that support alternate processing capabilities for NRC headquarters, found vulnerabilities that require remediation. Vulnerabilities were found in IT components owned by Region IV and NRC IT Infrastructure (ITI) components.[4] Vulnerabilities could result in disclosure of or unauthorized access to sensitive information, unauthorized privileged access, uploading unauthorized content, changing device configuration, and denial of service.

What Is Required

NIST SP 800-53, Revision 4, requires organizations to scan for vulnerabilities in information systems and remediate legitimate vulnerabilities within organization-defined response times. 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

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

one of the five keys tasks for continuous monitoring, as specified in ISD process 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 IV network, including the IRC network, the Region IV Resident Inspector sites, and some components that support alternate processing capabilities for NRC headquarters. All scan targets were physically located in Region IV and included IT components owned by Region IV, as well as components owned by the NRC ITI. Critical problems (high risk) and areas of concern (moderate risk) were identified.[5]

[5] Critical problems and areas of concern are the terms used by the tool used to perform the vulnerability scan.

Why This Is Important

Vulnerabilities could result in disclosure of or unauthorized access to sensitive information, unauthorized privileged access, uploading unauthorized content, changing device configuration, and denial of service.

RECOMMENDATION

OIG recommends that the Executive Director for Operations

3. Address the identified vulnerabilities within the timeframes specified in ISD standard ISD-STD-0020, *Organization Defined Values for System Security Controls*.

AGENCY COMMENTS

An exit conference was held with the agency on July 21, 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 four floors Region IV occupies at 1600 East Lamar Boulevard, Arlington, TX 76011-4511.

- Region IV seat-managed IT components and NRC-managed IT components.
- National security systems (including systems processing safeguards information) housed at Region IV.

The evaluation work was conducted during a site visit to Region IV in Arlington, TX, between July 17, 2017, and July 21, 2017. Any information received from NRC subsequent to the completion of fieldwork was incorporated into this report as appropriate. 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 the Region IV IRC, which includes several rooms housing national security systems (including systems processing safeguards information), and a room housing backup components for an NRC system located at NRC headquarters.

The team reviewed documentation provided by Region IV 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 IV Information Systems Security Officer (ISSO), alternate ISSO, server administrators, and other Region IV employees responsible for implementing the NRC IT security program at Region IV. The evaluation team also conducted user interviews with 15 Region IV employees, including 2 Resident Inspectors, and 7 teleworkers.

The information security risk evaluation also included a network vulnerability assessment scan of the Region IV network, including its IRC network, the Region IV Resident Inspector sites, and some components that support alternate processing capabilities for NRC headquarters. The evaluation team immediately notified Region IV of any critical vulnerabilities that were found. Subsequent to the completion of fieldwork, Region IV 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 ISD policies, processes, procedures, standards, and guidelines, and
- NRC OIG guidance.

The evaluation was conducted by Jane M. Laroussi, CISSP, and Diane Reilly, 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.