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

OFFICE OF THE
INSPECTOR GENERAL

May 2, 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 II, ATLANTA, GA (OIG-17-A-12)

The Office of the Inspector General (OIG) conducted this evaluation to perform an independent evaluation of NRC's implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for FY 2017 at NRC's Region II office and to evaluate the effectiveness of agency information security policies, procedures, and practices as implemented in this location. OIG found that backups for Region II servers are not being performed. Due to limited resources, Region II determined that efforts to support the deployment of the new Windows 2012 servers take precedence over repairing or replacing the backup server. The target deployment date for new servers is the end of April 2017. Therefore, OIG makes no recommendations.

BACKGROUND

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 II office oversees regulatory activities in the southeastern United States; is located in Atlanta, Georgia; 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…."

Region II Background

Region II is supported by information technology (IT) components that are seat-managed and that are NRC-managed. Seat-managed components provide core IT services at Region II, and include security appliances, routers, switches, servers (e.g., domain controllers, mail servers, file servers, multi-purpose servers, print servers), desktops, laptops, and printers. They are managed by NRC's seat-management contractor and are included in the authorization boundary of the IT Infrastructure (ITI) system. Additional IT components located in Region II are owned and managed by Region II and include a Web server, database servers, a backup server, and virtual servers. These components contain data utilized by the Region II IT staff for help desk management and computer imaging files. Data includes Web server data files, content, and configurations. Data for Region II NRC-managed servers are stored on a local storage area network (SAN) in a RAID 5 configuration.[3] NRC-managed servers at Region II are included in the authorization boundary of the Regional Information System – Region II Office (RIS-RII) Subsystem.

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 II office located in Atlanta, Georgia.

[3] RAID (redundant array of independent disks) is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purpose of data redundancy, performance improvement, or both. Data is distributed across the drives depending on the required level of redundancy and performance. RAID levels greater than RAID 0 provide protection against unrecoverable sector read errors, as well as against failures of whole physical drives. RAID 5 is a RAID configuration that uses disk striping with parity. Parity is an error protection scheme to provide fault tolerance in a given set of data. Because data and parity are striped across all disks, no single disk is a bottleneck. Striping also allows data to be reconstructed in case of disk failure.

OBJECTIVE

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

FINDING

Region II has continued to make improvements in its implementation of NRC's IT security program and practices for NRC IT systems since the previous evaluation in 2012. However, backups of Region II servers are not being performed.

Backups of Region II Servers Are Not Being Performed

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, backups of Region II servers are not being performed. As a result, Region II may not have reliable IT system backup information available if there is a need for system or file recovery.

What Is Required

NIST SP 800-53

NIST SP 800-53, 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. The specific backup methods and frequencies for NRC-managed servers in Region II are defined in the RIS-RII Subsystem System Security Plan.

Backups are copies of data, typically saved to magnetic disk, tape, or optical disks, such as compact disks (CDs), and often stored at an offsite location. They are an important part of contingency planning and are a means to restore system operations quickly and effectively following a service disruption.

What We Found

Backups of NRC-Managed Servers Are Not Being Performed

Approximately 2 months ago, Region II began experiencing hardware failures on the local backup server, which subsequently stopped working altogether. Region II decided not to attempt to repair the server, which is running the Windows 2003 Server operating system, as they are currently in the process of replacing all of their Windows 2003 servers with Windows 2012 servers. The target deployment date for the new servers is the end of April 2017. The Region II Administrator, who is the RIS-RII system owner, has accepted the business risk of not performing backups while the backup server is being replaced. There is some data redundancy since the server data is stored on the Region II SAN in the RAID 5 configuration.

Why This Occurred

Region II Backup Server Recently Failed

The age of the Windows 2003 backup server is the likely cause for the hardware failure. Due to limited resources, Region II determined that efforts to support the deployment of the new Windows 2012 servers take precedence over repairing or replacing the backup server.

Why This Is Important

Potential Risk of Data Loss

Backups ensure information necessary for operation 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. Unanticipated incidents, such as hard drive and other system failures, can result in devastating consequences if backup data is not available to restore operation.

There is a potential for data loss if the Region II SAN fails; however, Region II has accepted the business risk of not performing backups. As a result, Region II may not have reliable backup information available if there is a need for system or file recovery.

AGENCY COMMENTS

An exit conference was held with the agency on March 31, 2017. After this meeting, a discussion draft was provided to the agency for their comment. Agency management stated their general agreement with the finding and opted not to provide formal comments for inclusion in this report.

SCOPE AND METHODOLOGY

Scope

The scope of this evaluation included

- The six floors Region II occupies in the Marquis One Tower, 245 Peachtree Center Avenue N.E., Suite 1200, Atlanta, GA 30303-8931.
- Region II seat-managed IT components and NRC-managed IT components.
- National security systems (including systems processing safeguards information) housed at Region II.

The evaluation work was conducted during a site visit to Region II in Atlanta, GA, between March 27, 2017, and March 31, 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 were aware of the possibility of fraud, waste, and 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 a new room on the 8th floor that houses audio-visual equipment and a room housing national security systems (including systems processing safeguards information). The evaluation team also performed a spot check of two rooms previously surveyed in 2012 to confirm there have been no significant changes since 2012 and to confirm that a corrective action related to testing and monitoring of short-term uninterruptable power supplies is in place.

The team reviewed documentation provided by Region II 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 II Information Systems Security Officer, server administrators, and other Region II staff members responsible for implementing the NRC IT security program at Region II. The evaluation team also conducted user interviews with 15 Region II employees, including four Resident Inspectors 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.