EVALUATION REPORT

REDACTED FOR PUBLIC RELEASE

Information of Security Risk Evaluation of Region II – Atlanta GA

OIG-12-A-17   August 27, 2012

All publicly available OIG reports (including this report) are accessible through NRC's Web site at:
http:/www.nrc.gov/reading-rm/doc-collections/insp-gen/

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

OFFICE OF THE
INSPECTOR GENERAL

August 27, 2012

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: INFORMATION SECURITY RISK EVALUATION OF REGION II – ATLANTA, GA (OIG-12-A-17)

Attached is the Office of the Inspector General's (OIG) evaluation report titled, *Information Security Risk Evaluation of Region II - Atlanta, GA.*

The report presents the results of the subject evaluation. The agency agreed with the evaluation findings and did not provide comments at the July 13, 2012, exit conference.

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.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 415-5915 or Beth Serepca, Team Leader, Security and Information Management Team, at 415-5913.

Attachment: As stated

Information Security Risk Evaluation of Region II – Atlanta, GA

REDACTED FOR PUBLIC RELEASE

Contract Number: GS-00F-0001N
NRC Order Number: D12PD01191

August 22, 2012

The views, opinions, and findings contained in this report are those of the authors and should not be construed as an official Nuclear Regulatory Commission position, policy, or decision, unless so designated by other official documentation.

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

The U.S. Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) tasked Richard S. Carson & Associates, Inc. to perform an information security risk evaluation of the NRC's regional offices and the Technical Training Center. This report presents the results of the information security risk evaluation for Region II located in Atlanta, Georgia.

OBJECTIVES

The objectives of the Region II information security risk evaluation were to:

- Perform an independent information security risk evaluation of the NRC IT security program, policies, and practices for compliance with the Federal Information Security Management Act (FISMA) of 2002 in accordance with OMB guidance and Federal regulations and guidelines as implemented at Region II.
- Evaluate the effectiveness of agency security control techniques as implemented at Region II.

RESULTS IN BRIEF

Region II has made improvements in its implementation of NRC's IT security program and practices for NRC IT systems since the previous evaluations in 2003, 2006, and 2009. All corrective actions from the previous evaluations have been implemented. However, the Region II IT security program and practices are not always consistent with the NRC's IT security program, as summarized below.

Physical and Environmental Security Controls

All IT equipment in the Region II data center and telecommunications closets is connected to short-term uninterruptible power supplies (UPSs); however, the UPSs are not tested on a regular basis. As a result, Region II does not have assurance the UPSs will perform as expected in the event of a power failure. If a UPS fails during a power failure, equipment may not be shut down in an orderly manner, resulting in possible equipment damage or loss of data.

Region II key management procedures have not been fully implemented. [redacted]

[redacted]

Continuity of Operations and Recovery

Backup procedures are not maintained and kept up-to-date as required. As a result, Region II may not have reliable IT system backup information available if there is a need for system or file recovery.

IT Security Program

Some NRC-owned laptops have not been authorized to operate and documentation for regional laptop systems is not up-to-date. As a result, Region II is not fully compliant with NRC requirements for laptop systems. Without up-to-date documentation, Region II laptop systems users may not be aware of their responsibilities with regard to use of these laptops, which could lead to unauthorized use of NRC resources or release of sensitive information.

Regional IT security program procedures are not kept up-to-date. As a result, steps or processes could be skipped or forgotten if personnel responsible for a particular activity are unavailable. In addition, outdated procedures make it more difficult when training new personnel to handle a specific activity.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve NRC's information system security program and implementation of FISMA at Region II. A consolidated list of recommendations appears on page 15 of this report.

AGENCY COMMENTS

At an exit conference on July 13, 2012, agency officials agreed with the findings and did not provide any changes to the draft report. The agency opted not to submit formal comments.

ABBREVIATIONS AND ACRONYMS

CSO-STD	Computer Security Office Standard
FISMA	Federal Information Security Management Act
ISSO	Information Systems Security Officer
IRB	Information Resources Branch
IT	Information Technology
ITI	IT Infrastructure System
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
ROI	Regional Office Instruction
SGI	Safeguards Information
SP	Special Publication
UPS	Uninterruptible Power Supply

[Page intentionally left blank]

TABLE OF CONTENTS

[Page intentionally left blank]

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 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. The region covers a 10-State area, including 8 States with nuclear power plants. Region II also includes Puerto Rico and the U.S. Virgin Islands. Region II oversees commercial nuclear fuel processing facilities in Illinois and Ohio, which are located in Region III, as well as New Mexico and Washington, which are located in Region IV. Region II also handles all construction inspection activities for all new nuclear power plants and fuel cycle facilities, regardless of geographical location.

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, requires agencies to implement and maintain an information technology (IT) security program, including the preparation of policies, standards, and procedures. An effective IT security program is an important managerial responsibility. Management establishes a positive climate by making computer security a part of the information resources management process and by providing support for a viable IT security program.

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002.[1] FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[2] 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 compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines. FISMA requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor.[3]

NRC maintains an IT security program to provide appropriate protection of information resources. In this regard, the role of the NRC OIG is to provide oversight of agency programs,

[1] The Federal Information Security Management Act of 2002 was enacted on December 17, 2002, as part of the E-Government Act of 2002 (Public Law 107-347) and replaces the Government Information Security Reform Act, which expired in November 2002.

[2] 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 IT security program.

[3] 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 that "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…"

including the IT security program in support of the NRC goal to ensure the safe use of radioactive materials for beneficial civilian purposes while protecting people and the environment.

In support of its FISMA obligations, the NRC OIG tasked Richard S. Carson & Associates, Inc. to perform an information security risk evaluation of the NRC's regional offices and the Technical Training Center to evaluate IT security programs in place at those locations, to include an assessment of physical security weaknesses in protecting the IT security program, and to identify existing problems and make recommendations for corrective actions.

The information security risk evaluation focused on the following elements of the NRC's IT security program, policies, and practices:

- Physical and Environmental Security Controls.
- Logical Access Controls.
- Configuration Management.
- Continuity of Operations and Recovery.
- IT Security Program.

This report presents the results of the information security risk evaluation for Region II. A consolidated list of recommendations appears on page 15.

2 Objectives

The objectives of the Region II information security risk evaluation were to:

- Perform an independent information security risk evaluation of the NRC IT security program, policies, and practices for compliance with FISMA in accordance with OMB guidance and Federal regulations and guidelines as implemented at Region II.
- Evaluate the effectiveness of agency security control techniques as implemented at Region II.

The appendix contains a description of the evaluation objectives, scope, and methodology.

3 Findings

Region II has made improvements in its implementation of NRC's IT security program and practices for NRC IT systems since the previous evaluations in 2003, 2006, and 2009. All corrective actions from the previous evaluations have been implemented. However, the Region II IT security program and practices are not always consistent with the NRC's IT security program as defined in Management Directive (MD) and Handbook 12.5, *NRC Automated Information Systems Security Program*, other NRC policies, FISMA, and National Institute of Standards and Technology (NIST) guidance. While many of the Region II automated and manual IT security controls are generally effective, some IT security controls need improvement.

Specifics on physical and environmental security controls, continuity of operations and recovery, and the Region II IT security program are described in the following sections.

3.1 Physical and Environmental Security Controls

Overall, Region II is implementing the physical and environmental security controls described in MD and Handbook 12.1, *NRC Facility Security Program*; MD and Handbook 12.5; and NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. Region II has implemented a number of safeguards to restrict access to the facility, including visitor access controls and physical access control systems. Fire suppression and detection systems are adequate and meet NRC requirements. Environmental controls are sufficient to protect IT equipment from potential hazards. Short-term uninterruptible power supplies (UPSs) provide sufficient power to facilitate an orderly shutdown of IT equipment in the event of a primary power source loss. However, the evaluation team identified issues with testing UPSs and key and combination management procedures.

FINDING #1: UPSs Are Not Tested on a Regular Basis

NIST SP 800-53, physical and environmental control PE-11, emergency power, states that organizations should provide a short-term UPS to facilitate an orderly shutdown in the event of a primary power source loss. All IT equipment in the Region II data center and telecommunications closets is connected to short-term UPSs; however, the UPSs are not tested on a regular basis. As a result, Region II does not have assurance the UPSs will perform as expected in the event of a power failure. If a UPS fails during a power failure, equipment may not be shut down in an orderly manner, resulting in possible equipment damage or loss of data.

3.1.1 Emergency Power Requirements

NIST SP 800-53, physical and environmental control PE-11, emergency power, states that organizations should provide a short-term UPS to facilitate an orderly shutdown in the event of a primary power source loss.

3.1.2 Agency Has Not Fully Met Requirements

All IT equipment in the Region II data center and telecommunications closets are connected to short-term UPSs. However, the UPSs are not tested on a regular basis to ensure they are operating and can provide the requisite amount of power necessary to facilitate an orderly shutdown of equipment in the event of a primary power source loss. One of the assumptions in developing the contingency plan for the Region II Office Support System is that data center equipment is connected to UPSs that provide approximately 20 minutes of electricity during a power failure.

3.1.3 Impact on Region II Operations

While NIST and NRC do not explicitly require periodic testing of UPSs, if UPSs are not periodically tested, Region II does not have assurance the UPSs will perform as expected in the event of a power failure. If a UPS fails during a power failure, equipment may not be shut down in an orderly manner, resulting in possible equipment damage or loss of data.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Develop, document, and implement procedures for testing UPSs on a periodic basis. Procedures should include a means to record the results of such testing.

3.1.4 Physical Access Control Systems

On April 12, 2010, the Region II office moved to 245 Peachtree Center Ave, NE, Atlanta, GA. These facilities were specifically constructed based upon Region II needs and requirements. One of the major requirements was to significantly reduce the number of keyed doors, instead selecting to use electronic access controls. As a result of these requirements, the use of keyed doors has been greatly reduced. [redacted][4] [redacted]

- [redacted]
- [redacted]
- [redacted]

FINDING #2: Key and Combination Management Procedures Need Improvement

MD and Handbook 12.5 provide guidance for key and combination control procedures, including the requirement to establish, document, implement, and enforce effective key and combination control procedures. However, Region key management procedures have not been fully implemented. [redacted]

[4] [redacted]

[redacted]

3.1.5 Physical Access Requirements

MD and Handbook 12.5 provide guidance for key and combination control procedures, including the requirement to establish, document, implement, and enforce effective key and combination control procedures. Offices are required to create a comprehensive inventory of all keys and combinations related to the security of office areas, systems equipment, and sensitive areas. The inventory should include the room number, number of keys, names of individual(s) issued to, and date issued. Periodic inventories of all keys should be conducted and recorded and inventories should be maintained as official records for 1 year after they are no longer current.

[redacted]

3.1.6 Agency Has Not Fully Met Requirements

Region II developed the *Region II Information Resources Branch Standard Operating Procedure – Key Inventory Process* as a result of a recommendation from OIG’s 2009 Region II computer security review. This procedure documents key management activities including distribution of keys, replacement keys, other lock and key work, return of keys, and conducting periodic key inventories. As part of an internal assessment, Region II has acknowledged that its key management procedures have not been fully implemented. [redacted] Region II has initiated an internal action item using its ticketing system to correct problems identified with its key management process. [redacted]

[redacted]

3.1.7 Impact on Region II Operations

[redacted] For example, a key could be issued without recording information about who was issued the key and when. Documenting these procedures helps ensure that there is continuity in the key and combination management process in the event of staff turnover. Additionally, documented procedures are excellent for training new personnel and an excellent reference for existing personnel. [redacted]

MD and Handbook 12.5 require combinations to be changed immediately when individuals no longer have a need for access. [redacted]

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

2. Update key management procedures. [redacted]
3. Develop, document, and implement combination management procedures. [redacted]
   a) [redacted]
   b) [redacted]

3.2 Continuity of Operations and Recovery

Region II procedures for maintaining continuity of operations and recovery are generally consistent with the requirements in MD and Handbook 12.1, MD and Handbook 12.5, NRC standards, and NIST SP 800-53. Region II has documented procedures for backups of seat-managed servers, backups of NRC-managed servers, and for offsite backup storage. Region II has also developed a site-specific Occupant Emergency Plan and a contingency plan for the Region II Office Support System.

However, the evaluation team found that backup procedures are not maintained and kept up-to-date as required. As a result, Region II may not have reliable IT system backup information available if there is a need for system or file recovery.

3.2.1 Region II Servers

Region II is supported by IT equipment that is seat-managed and that is NRC-managed. Core regional servers are provided and managed by the seat management contractor and include domain controllers, mail servers, multipurpose servers, a tape server, and virtual servers. These systems contain data utilized by the IT staff, customer data, e-mail accounts, backup tape server database files and access control. IT staff data includes software packages, workstation images, Web content, videocast files, and IT shared content. Customer data includes division-shared folders, personal folders, and other files/folders accessed via regional network mapped shares. Seat-managed servers are included in the authorization boundary of the IT Infrastructure (ITI) system. Additional regional servers are owned and managed by Region II and include a Web server, database servers, a backup server, and virtual servers. These systems contain data utilized by the IT staff for help desk management and computer imaging files. Data includes Web server data files, content, and configurations. The data also includes any associated scripting engines or applications related to the Web server and its configurations. NRC-managed servers at Region II are included in the authorization boundary of the Region II Office Support System.

FINDING #3: Backup Procedures Are Not Up-to-Date

MD and Handbook 12.5, NRC standards, and NIST SP 800-53 detail requirements for backups of IT systems. However, Region II has not met all the requirements. Specifically, backup procedures are not maintained and kept up-to-date as required. As a result, Region II may not have reliable IT system backup information available if there is a need for system or file recovery.

3.2.2 Backup Requirements

MD and Handbook 12.5 detail requirements for backups of IT systems, and states that these procedures should be implemented when backing up media to ensure that reliable backups are available if there is a need for system or file recovery. These procedures include, but are not limited to:

- Backup schedule – outlines the type of backup, the interval for each backup, the storage location, and the number of copies of each backup.
- Full backups – performed at least weekly.
- Incremental (differential) backups – performed nightly.
- Location of backups – at least two full backups maintained. One should remain onsite and a second copy should be removed to an offsite storage facility immediately after its creation.

- Backup media – use high-quality media to ensure good quality backups are available for recovery should the need arise.
- Storage of backups – store both onsite and offsite backups in a location, cabinet, or safe that is waterproof and fireproof for at least 14 days or as recommended by the agency.
- Testing of storage – backups are periodically tested to ensure they can be used effectively to restore sensitive information.

CSO-STD-2002, *System Back-up Standard*, V1.1, dated December 15, 2010, states backup and recovery procedures are to be developed, documented, approved, maintained, and used for all systems operated by or on behalf of NRC.

3.2.3 Agency Has Not Fully Met Requirements

Region II has developed backup procedures for both seat-managed servers and NRC-managed servers. These procedures are documented in the Information Resources Branch (IRB)-IT-03 *GFE and Contractor Leased Server Backup Procedures*, dated March 31, 2011, as well as in separate documents maintained by the seat-management server administrator and the Region II server administrator. As a result of a recommendation from OIG's 2009 Region II computer security review, Region II developed the *Region II Information Resources Branch Standard Operating Procedure Region II Offsite Backup Storage Procedures*.

While Region II has developed and documented required backup procedures, there was confusion as to whether the IRB-IT-03 document with the combined procedures was the "official" version, or if the separately maintained procedures should be considered official versions. The procedures for backups of NRC-managed servers are the same in the IRB-IT-03 document and in the separate document maintained by the Region II server administrator. However, the procedures for backups of seat-managed servers in the IRB-IT-03 document were not current and differed from those in the separate document maintained by the seat-management server administrator. The procedures in the separate document maintained by the seat-management server administrator are current; however, they do not contain the same level of detail as in the older content found in the IRB-IT-03 document, such as a description of the backup software used, license information for the backup software, a description of the tape library, a description of the backup job, the account used to run the backup jobs, and a summary of data on each server. The seat-management server administrator also maintains a monthly image of the Citrix servers on the behalf of ITI; however, this process is not documented in any procedures. The Region II server administrator also mentioned the use of shadow copies to facilitate rapid restores without having to get backup tapes from offsite storage; however, this process is also not documented in any procedures.

The *Region II Offsite Backup Storage Procedures* describes the procedures for sending backups of seat-managed and NRC-managed servers to an offsite location; however, this document refers to outdated versions of backup procedures for these servers.

3.2.4 Potential Risk of Data Loss

While the backup procedures that are currently implemented would minimize data loss in the event of a computer failure, the procedures are not maintained and kept up-to-date as required. Software performs many of the backups automatically, but someone must periodically change the tapes. The procedures need to be fully documented so that if the primary personnel responsible for backups are unavailable, alternates have the information necessary to follow the procedures. Current and fully documented backup procedures can also be useful when training new employees with responsibilities for performing backups.

As a result of the failure to meet agency and NIST requirements regarding backups of IT systems, Region II may not have reliable IT system backup information available if there is a need for system or file recovery.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

4. Update backup procedures for NRC-managed servers to include procedures for maintaining shadow copies to support the backup process.
5. Update backup procedures for seat-managed servers to include the same level of detail as in the backup procedures for NRC-managed servers and procedures for maintaining a monthly image of the Citrix servers on the behalf of ITI.
6. Update offsite backup storage procedures to include correct references to the backup procedures for seat-managed and NRC-managed servers.

3.3 Information Technology Security Program

Overall, Region II is following agency security policies and procedures regarding IT security. Region II has developed regional office instructions that are generally up-to-date and are available on the Region II internal Web site. Staff receive training regarding IT security during the onboarding process and the Information Systems Security Officer (ISSO) sends periodic cybersecurity reminders on topics. Users are generally aware of and are following agency and Region II IT security policies and procedures. Region II maintains an inventory of IT systems in use at the region, to include a general support system, two subsystems (applications), and laptops processing safeguards information (SGI) and classified information.

However, the evaluation team found issues with the Region II laptop systems and with keeping Region II IT security program procedures up-to-date.

3.3.1 Region II Laptop Systems

Laptops in use at Region II are either seat-managed laptops or NRC-owned laptops. Seat-managed laptops in use at Region II include those laptops that are part of the agency's new *work from anywhere/mobile desktop program*. NRC-owned laptops in use at Region II include loaner laptops, stationary laptops found in conference rooms, and laptops used to process classified information or SGI.

FINDING #4: Some Laptops Are Not Authorized To Operate and Documentation for Regional Laptop Systems Is Not Up-to-Date

The *NRC Laptop Security Policy*, which specifies the requirements for authorization of laptop systems, states that all NRC laptops must be either designated a system or included as part of an existing system. NRC-owned laptops in use at Region II include loaner laptops, stationary laptops found in conference rooms, and laptops used to process classified information or SGI. However, the evaluation team found that some NRC-owned laptops have not been authorized to operate and documentation for regional laptop systems is not up-to-date. As a result, Region II is not fully compliant with NRC requirements for laptop systems. Without up-to-date documentation, Region II laptop systems users may not be aware of their responsibilities with regard to use of these laptops, which could lead to unauthorized use of NRC resources or release of sensitive information.

3.3.2 Laptop System Requirements

The *NRC Laptop Security Policy* states that all NRC laptops must either be designated a system or be included as part of an existing system. All laptops that are not seat-managed are considered to be organization-managed, i.e., NRC-owned. All NRC-owned laptops that process or access classified national security information belong to that office or region’s “Classified Laptop System.” All NRC-owned laptops that process or access SGI and are not part of the office or region’s “Classified Laptop System” belong to that office or region’s “SGI Laptop System.” All NRC-owned laptops that are not part of the office or region’s “Classified Laptop System” or the office or region’s “SGI Laptop System” belong to that office or region’s “General Laptop System.”

The *NRC Laptop Security Policy* also specifies the following requirements for authorization (formerly referred to as accreditation):

- Laptop systems must meet the requirements provided in the relevant standard security plan. There is a different standard security plan for classified, SGI, and general laptops.
- Laptop systems must be certified by the system owner as compliant with the relevant laptop system requirements.
- Laptop systems must be accredited by the appropriate Designated Approving Authority prior to processing any relevant (i.e., classified, SGI, sensitive unclassified) information on the system.
- Certification of a laptop system requires a system certification memorandum from the laptop system owner. The memorandum must include an enclosure that provides the names and contact information for the: System Owner, Certification Agent, ISSO, Alternate ISSO, and System Administrator.

- For each laptop or removable hard drive that is part of the laptop system, the enclosure must provide information such as physical storage location, location where system is used, brand, model, tag number, peripherals, etc.

3.3.3 Agency Has Not Fully Met Requirements

Region II currently has two laptop systems – a classified laptop system (currently two laptops) and an SGI laptop system. The SGI laptop system consists of two separate subsystems – SGI laptops in use in the Region II office (currently four laptops), and SGI laptops in use at the Resident Inspector sites (multiple laptops, recently replaced by Safeguards Information Local Area Network and Electronic Safe workstations). In 2009, Region II submitted certification memoranda and the required enclosure for authorization of the following laptop systems. These systems were authorized to operate until August 2012.

- Region II Classified Laptop System (2 laptops).
- Region II SGI Standalone Personal Computer System (four laptops).
- Region II SGI Laptop System (laptops at Resident Inspector sites).

Region II is currently in the process of replacing the two classified laptops with four new units and the two SGI laptops with two new units.

Some Laptops Are Not Authorized To Operate

Region II has not established a general laptop system, which would include its loaner laptops and stationary laptops found in conference rooms. Region II is evaluating whether to continue to manage these laptops as NRC-owned laptops, or to replace them with seat-managed laptops. If Region II decides to continue to manage these laptops as NRC-owned laptops, then Region II will need to establish a general laptop system and complete the process described in the *NRC Laptop Security Policy* for authorization of the general laptop system.

Documentation for Regional Laptop Systems Is Not Up-to-Date

The following Regional Office Instructions (ROI) have been issued to provide an overview of the security requirements, description of security controls, and delineation of the responsibilities and expected behavior of all individuals who use laptops that process classified and SGI information:

- ROI No. 1251, Revision 1, Region II System Security Plan for Processing Classified Information, dated June 4, 2012.
- ROI No. 1250.1, Region II System Security Plan for Processing Safeguards Information (Laptop Computer System), dated September 10, 2003.
- ROI No. 1250.2, Region II System Security Plan for Processing Safeguards Information (Removable Hard Drive System), dated September 2003.

ROI No. 1251, Revision 1, corresponds to the four new classified units currently awaiting authorization to operate. The previous version of ROI No. 1251, dated September 26, 2003, corresponded to the two classified laptops currently authorized to operate. However, ROI No. 1250.1 and 1250.2 do not correspond to either of the SGI laptop systems (the four laptops in use at the Region II office and the laptops recently removed from the Resident Inspector sites) currently authorized to operate.

3.3.4 Impact on Region II Operations

While Region II has followed the procedures in the *NRC Laptop Security Policy* for authorization of its classified and SGI laptop systems, it has not followed this process for authorization of the general laptop system. In addition, Region II has not kept the ROIs up-to-date that correspond to the different laptop systems. As a result, Region II is not fully compliant with NRC requirements for laptop systems. Without up-to-date documentation, Region II laptop systems users may not be aware of their responsibilities with regard to use of these laptops, which could lead to unauthorized use of NRC resources or release of sensitive information.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

7. Establish a general laptop system and complete the process described in the *NRC Laptop Security Policy* for authorization of the general laptop system.
8. Update ROI 1250.1/1250.2 to correspond to the SGI laptop systems in use at Region II and currently authorized to operate.

3.3.5 Regional Procedures and Instructions

Region II uses various types of procedures to implement their IT security program. These procedures include standard operating procedures issues by the Division of Resource Management and Administration Information Resources Branch and ROI. Standard operating procedures are used to describe specific activities, such as key and keycard management and performing backups. ROI are typically used to disseminate, implement, clarify, or amplify policy or other information contained in other NRC documents. For example, Region II uses ROI to communicate various aspects of the Region II security program, including personnel security, facility security, telecommunications security, and security for sensitive, SGI, and classified information.

FINDING #5: Regional IT Security Program Procedures Are Not Kept Up-to-Date

NRC has developed several security standard that specify the frequency of reviewing and updating IT security program procedures. However, as discussed in finding 2, 3, and 4, regional IT security program procedures are not kept up-to-date. As a result, steps or processes could be skipped or forgotten if personnel responsible for a particular activity are unavailable. In addition, outdated procedures make it more difficult when training new personnel to handle a specific activity.

3.3.6 Requirements for Updating Procedures

CSO-STD-0020, defines the mandatory values for specific controls in the eighteen security controls families described in NIST SP 800-53. The standard requires that documented procedures to facilitate the implementation of a control should be reviewed and updated annually. The standard also requires system owners to review system security plans at least annually and update them to address changes to the information system and/or environment of operation. CSO-STD-2001, *Operating Procedures Standard*, V1.1, dated April 15, 2011, 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.

3.3.7 Agency Has Not Fully Met Requirements

Region II has documented procedures to facilitate the implementation of specific IT security controls, including key management, performing backups, and security for sensitive, SGI, and classified information. However, as discussed in findings 2, 3, and 4, the evaluation team found that several of these procedures are not up-to-date.

Region II does not have a process for reviewing and updating procedures on a periodic basis. ROI No. 0201, Revision 9, *System of Instructions and Notices*, dated March 19, 2012, describes the process for issuing ROIs; however, it does not specify the frequency for which ROIs should be reviewed to determine if they require updates.

3.3.8 Impact on Region II Operations

Outdated procedures can result in steps or processes being skipped or forgotten if personnel responsible for a particular activity are unavailable. In addition, outdated procedures make it more difficult when training new personnel to handle a specific activity. In the case of the outdated ROIs, Region II is not in compliance with NRC requirements for laptop systems. Without up-to-date procedures, Region II laptop systems users may not be aware of their responsibilities with regard to use of these laptops. Current procedures ensure continuity in performing a specific IT security function in the event of staff turnover and are excellent for training new personnel and an excellent reference for existing personnel.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

9. Develop, document, and implement a procedure for reviewing and updating IT security program procedures, including regional office instructions, on an annual basis.

[Page intentionally left blank]

4 Consolidated List of Recommendations

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Develop, document, and implement procedures for testing UPSs on a periodic basis. Procedures should include a means to record the results of such testing.
2. Update key management procedures. [redacted]
3. Develop, document, and implement combination management procedures. [redacted]
   a) [redacted]
   b) [redacted]
4. Update backup procedures for NRC-managed servers to include procedures for maintaining shadow copies to support the backup process.
5. Update backup procedures for seat-managed servers to include the same level of detail as in the backup procedures for NRC-managed servers and procedures for maintaining a monthly image of the Citrix servers on the behalf of ITI.
6. Update offsite backup storage procedures to include the correct references to the backup procedures for seat-managed and NRC-managed servers.
7. Establish a general laptop system and complete the process described in the *NRC Laptop Security Policy* for authorization of the general laptop system.
8. Update ROI 1250.1/1250.2 to correspond to the SGI laptop systems in use at Region II and currently authorized to operate.
9. Develop, document, and implement a procedure for reviewing and updating IT security program procedures, including regional office instructions, on an annual basis.

[Page intentionally left blank]

5 Agency Comments

At an exit conference on July 13, 2012, agency officials agreed with the findings and did not provide any changes to the draft report. The agency opted not to submit formal comments.

[Page intentionally left blank]

Appendix. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The objectives of the Region II information security risk evaluation were to:

- Perform an independent information security risk evaluation of the NRC computer security program, policies, and practices for compliance with FISMA in accordance with OMB guidance and Federal regulations and guidelines as implemented at Region II.
- Evaluate the effectiveness of agency security control techniques as implemented at Region II.

SCOPE

The scope of this information system security 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 equipment.
- Region II NRC-managed equipment.

The information system security evaluation did not include controls related to the management of safeguards or classified information.

The evaluation work was conducted during a site visit to Region II in Atlanta, GA, between July 9, 2012, and July 13, 2012. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible. Throughout the evaluation, evaluators were aware of the potential for fraud, waste, or misuse in the program.

METHODOLOGY

Richard S. Carson & Associates, Inc. conducted a high-level, qualitative evaluation of NRC computer security program, policies, and practices as implemented at Region II, and evaluated the effectiveness of agency security control techniques as implemented at Region II.

In conducting the information security risk evaluation, the following areas were reviewed: physical and environmental security controls, logical access controls, configuration management, information system security program, and continuity of operations and recovery. Specifically, the evaluation team conducted site surveys of the six floors Region II occupies in the Marquis One Tower, 245 Peachtree Center Avenue N.E., Suite 1200, Atlanta, GA 30303-8931, focusing on the areas that house IT equipment. The team conducted interviews with the Region II ISSO, the seat-management server administrator, the Region II server administrator, and other Region II staff members responsible for implementing the agency's information system security program at Region II. The evaluation team also conducted user interviews with 15 Region II employees, including two Resident Inspectors and one teleworker. The team reviewed documentation provided by Region II including floor plans; inventories of IT systems, hardware, and software; local policies and procedures; security plans; backup procedures; contingency plans, and the Occupancy Emergency Plan. The information security risk evaluation also included a network vulnerability assessment scan of the Region II network and the Region II Resident Inspector sites.

All analyses were performed in accordance with guidance from the following:

- NIST standards and guidelines.
- NRC MD and Handbook 12.5, *NRC Automated Information Security Program*.
- NRC Computer Security Office policies, processes, procedures, standards, and guidelines.
- NRC OIG audit guidance.

The work was conducted by Jane M. Laroussi, CISSP, CAP, GIAC ISO-17799; Virgil Isola, CISSP; and Joseph Rood, GWAPT, CISSP, CISA, from Richard S. Carson & Associates, Inc.