EVALUATION REPORT

Information Security Risk Evaluation of Region III – Lisle, IL

OIG-12-A-22 September 26, 2012

OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

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

OFFICE OF THE
INSPECTOR GENERAL

September 26, 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 III – LISLE, IL (OIG-12-A-22)

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

The report presents the results of the subject evaluation. The agency agreed with the evaluation findings at the August 10, 2012, exit conference, and provided comments on September 25, 2012, which were incorporated, as appropriate, into this report.

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 III – Lisle, IL

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

September 25, 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 tasked Richard S. Carson & Associates, Inc., to perform an information security risk evaluation of NRC's regional offices and the Technical Training Center. This report presents the results of the information security risk evaluation for the Region III office, which is located in Lisle, Illinois.

OBJECTIVES

The Region III information security risk evaluation objectives were to:

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

RESULTS IN BRIEF

Region III 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 III IT security program and practices are not always consistent with NRC's IT security program, as summarized below.

Continuity of Operations and Recovery

Server administration procedures, including backup procedures are not maintained and kept up-to-date as required.

IT Security Program

Regional procedures and divisional instructions specific to the Region III IT security program 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 IT security program and implementation of FISMA at Region III. A consolidated list of recommendations appears on pages 11 of this report.

ABBREVIATIONS AND ACRONYMS

ATO	Authority to Operate
CSO-STD	Computer Security Office Standard
FISMA	Federal Information Security Management Act
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network
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
RP	Regional Procedure
SGI	Safeguards Information
SP	Special Publication

[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 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. The region covers a seven-State area, including six States with nuclear power plants. Region III also oversees materials licensees in Missouri, which is located in Region IV.

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 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 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, 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.

[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, "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…"

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

The information security risk evaluation focused on the following elements of 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 III. A consolidated list of recommendations appears on page 11.

2 Objectives

The Region III information security risk evaluation objectives 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 III.
- Evaluate the effectiveness of agency security control techniques as implemented at Region III.

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

3 Findings

Region III 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 III IT security program and practices are not always consistent with 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 III automated and manual IT security controls are generally effective, some IT security controls need improvement. Specifics on continuity of operations and recovery and the Region III IT security program are described in the following sections.

3.1 Continuity of Operations and Recovery

Region III procedures for maintaining continuity of operations and recovery are generally consistent with the requirements 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 III has documented server administration procedures, including procedures for backups of seat-managed and NRC-managed servers. Region III has also developed a site-specific Occupant Emergency Plan and a contingency plan for the Region III Private Branch Exchange.

However, the evaluation team found that server administration procedures, including backup procedures, are not maintained and kept up-to-date as required.

3.1.1 Region III Servers

Region III is supported by IT equipment that is both seat-managed and 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. Seat-managed servers are included in the authorization boundary of the IT Infrastructure system. Additional regional servers are owned and managed by Region III and include a database server and knowledge management servers. NRC-managed servers at Region III are included in the authorization boundary of the Region III Site System.

FINDING #1: Server Administration Procedures Are Not Up-to-Date

MD and Handbook 12.5, NRC standards, and NIST SP 800-53 detail requirements for certain aspects of server administration, including backups of IT systems. However, Region III has not met all the requirements. Specifically, server administration procedures, including backup procedures, are not maintained and kept up-to-date as required.

3.1.2 Server Administration 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.

Computer Security Office Standard (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.

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.

3.1.3 Agency Has Not Fully Met Requirements

Region III has developed server administration procedures, including backup procedures, for both seat-managed servers and NRC-managed servers. These procedures are documented in DI-NR-008, *Server Administration*, dated September 10, 2010. The seat-management contractor is responsible for performing backups of both seat-managed and NRC-managed serves. While Region III has developed and documented required backup procedures, the procedures do not reflect the server infrastructure currently in place in Region III. For example, DI-NR-008 includes a list of seat-managed and NRC-managed servers covered by the document; however, this list includes several servers that have been decommissioned and does not include several new servers. In addition, DI-NR-008 states that all servers listed Section C of the document are included in the backup procedures when, in fact, they are not. The Region III seat-management contractor is not responsible for performing backups of the Citrix servers located in Region III. In addition, the seat-management contractor is frequently asked by headquarters to create a Ghost[4] image of a server that headquarters needs to patch (e.g., Citrix server, badge access system server). This process is currently ad hoc and there is no set schedule. In addition, procedures for creating Ghost images, including where those images are stored, are not documented.

In addition to outdated backup procedures, DI-NR-008 also includes references to the previous seat-management contractor. The seat-management contract was transitioned to the current contractor in December 2011. This document also includes a section describing role-based access to Region III servers; however, this section is not up-to-date and does not reflect the current server infrastructure in place in Region III.

[4] Ghost (general hardware-oriented system transfer) is a software product that creates full system (disk image) backups.

3.1.4 Impact on Region III Operations

While the server administration procedures that are currently implemented would ensure server availability during core hours and minimize data loss in the event of a computer failure, the procedures are not up-to-date. For example, software performs many of the backups automatically, but someone must ensure the backup jobs include all required servers and run without errors. The procedures need to be 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

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

1. Update DI-NR-008, *Server Administration*, to (i) reflect the current Region III server infrastructure; (ii) document current backup procedures for seat-managed and NRC-managed servers; (iii) document procedures for creating Ghost images, including where those images are stored; (iv) define the schedule for creating Ghost images; (v) correct references to the current seat-management contractor; and (vi) correct any other sections impacted by the changes to the server infrastructure or the transition to the new seat-management contractor.

3.2 Information Technology Security Program

Overall, Region III is following agency security policies and procedures regarding IT security. Region III has developed regional procedures and divisional instructions that are generally up-to-date and are available on the Region III 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 III IT security policies and procedures.

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

3.2.1 Region III Laptop Systems

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

FINDING #2: Some Laptops Do Not Have a Current Authority To Operate

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 III include loaner laptops and laptops used to process SGI or classified information. However, the evaluation team found that some NRC-owned laptops do not have a current authority to operate (ATO). As a result, Region III is not fully compliant with NRC requirements for laptop systems.

3.2.2 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's or region's "Classified Laptop System." All NRC-owned laptops that process or access SGI and are not part of the office's or region's "Classified Laptop System" belong to that entity's "SGI Laptop System." All NRC-owned laptops that are not part of the office's or region's "Classified Laptop System" or the office's or region's "SGI Laptop System" belong to that entity'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.

3.2.3 Agency Has Not Fully Met Requirements

Region III currently has one laptop system – a general laptop system with a current ATO that covers the Region III loaner laptops. Region III also has three SGI laptops still on the NRC inventory of systems. During the site visit to Region III, the evaluation team was unable to determine whether the three SGI laptops were still in use and therefore should be covered under a Region III SGI laptop system with a current ATO. Subsequent to the site visit, Region III informed the evaluation team the three SGI laptops are no longer in use and are in the process of being decommissioned. Therefore, there is no need for Region III to establish a Region III SGI laptop system to cover these three laptops.

3.2.4 Regional Procedures and Instructions

Region III uses various types of procedures to inform the staff of standardized regional practices, division-level directives related to policy and operational matters, and general information, including policies, practices, and guidance specific to the Region III IT security program. These procedures include regional procedures, regional notices, and division instructions. Regional procedures are policies, practices, or guidance affecting more than one division or programmatic area within the regional office or programs in more than one strategic arena. They are intended to be of a permanent or long-term nature and remain in effect until they are revised or cancelled. Regional notices are intended to keep the staff informed, but do not establish comprehensive policy for the staff to follow. All notices contain an expiration date. Division instructions are policies, practices, or guidance affecting one division or programmatic area and are used to disseminate detailed guidance at the division level for implementing procedures or other agency policy.

The following are some examples of regional procedures and divisional instructions specific to the Region III IT security program:

- RP-12.1, *Region III Facility Security Program*, dated October 8, 2010 – describes the policies, controls, and employee responsibilities for the protection of Region III personnel, property, and unclassified facilities.
- DI-12.1, *Region III Security System Testing Process*, dated January 4, 2012 – provides guidance and instructions related to the processes necessary for Region III to perform NRC-required security system tests.
- DI-12.1, *Badging Procedures*, dated April 27, 2012 – provides details and procedures for enrolling, obtaining, activating, distributing, and monitoring security badges in NRC Region III office space.
- DI-NR-006, *Region III Switchboard Operations*, dated October 20, 2010 – a procedure and handbook that establishes and provides guidance for contractors and NRC personnel responsible for day-to-day operations of the Region III switchboard and reception area.
- DI-NR-008, *Server Administration*, dated September 10, 2010 – provides a standardized mode of operation to support the network servers used in Region III.

FINDING #3: Regional IT Security Program Procedures Are Not Kept Up-to-Date

NRC has developed several security standards that specify the frequency of reviewing and updating IT security program procedures. However, as discussed in finding 1 and further described in the following sections, regional procedures and divisional instructions specific to the Region III IT security program 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.

3.2.5 Requirements for Updating Procedures

CSO-STD-0020, *Organization Defined Values for System Security Controls*, Revision 1.1, dated July 1, 2012, defines the mandatory values for specific controls in the 18 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 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.

Regional Procedure (RP) 3.57, *System of Procedures, Notices, and Division Instructions*, dated October 15, 2009, controls activities associated with the development, revision, and cancellation of regional procedures, regional notices, and division instructions in sufficient detail to ensure processing standardization. RP-3.57 requires procedures and instructions to be reviewed or revised, at a minimum, every 3 years.

3.2.6 Agency Has Not Fully Met Requirements

Region III has developed several regional procedures and divisional instructions specific to the Region III IT security program. However, as discussed in finding 1, the evaluation team found that DI-NR-008 is not up-to-date. In addition, the evaluation team found that the following regional procedures and divisional instructions are also not up-to-date:

- RP-12.1, *Region III Facility Security Program* – Section F.4.h describes the requirement to review access permissions to the Region III server room and local area network (LAN) closets (that are equipped with card readers) on a semiannual basis. However, this process is now performed quarterly as part of the testing of the Region III security system. In addition, sections F.4.c and F.4.f of this document describe the old color-coded NRC identification badges.
- DI-12.1, *Region III Security System Testing Process* – as of June 2012, the quarterly security system test also includes a review of access permissions to the Region III server room and LAN closets (that are equipped with card readers). This document does not describe the process for performing that review.
- DI-NR-006, *Region III Switchboard Operations* – section IV.B.3 of the handbook describes the old color-coded NRC identification badges. Some of the functions described in this document are now performed by the protective security officer (e.g., performing an audit of all temporary badges); however, this document assigns those duties to the receptionist.

RP-3.57 requires procedures and instructions to be reviewed or revised, at a minimum, every 3 years. However, per NRC security standards, some procedures require more frequent review and update – at least annually for documented procedures to facilitate the implementation of security controls in the 18 security controls families described in NIST SP 800-53 and for operational procedures that capture the requirements for secure operation of information systems and for effective management and support of IT systems.

3.2.7 Impact on Region III 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. 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.

RECOMMENDATIONS

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

2. Update RP-12.1, *Region III Facility Security Program*, to describe the current requirement to review access permissions to the Region III server room and LAN closets (that are equipped with card readers) on a quarterly basis and to reflect the current NRC employee badge characteristics.
3. Update DI-12.1, *Region III Security System Testing Process*, to describe the current requirement to review access permissions to the Region III server room and LAN closets (that are equipped with card readers) on a quarterly basis.
4. Update DI-NR-006, *Region III Switchboard Operations,* to reflect the current NRC employee badge characteristics and to describe functions now performed by the protective security officer instead of the receptionist.
5. Update RP-3.57, *System of Procedures, Notices, and Division Instructions*, to specify which regional procedures and divisional instructions require annual review and update.

[Page intentionally left blank]

4 Consolidated List of Recommendations

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

1. Update DI-NR-008, *Server Administration*, to (i) reflect the current Region III server infrastructure; (ii) document current backup procedures for seat-managed and NRC-managed servers; (iii) document procedures for creating Ghost images, including where those images are stored; (iv) define the schedule for creating Ghost images; (v) correct references to the current seat-management contractor; and (vi) correct any other sections impacted by the changes to the server infrastructure or the transition to the new seat-management contractor.
2. Update RP-12.1, *Region III Facility Security Program*, to describe the current requirement to review access permissions to the Region III server room and LAN closets (that are equipped with card readers) on a quarterly basis and to reflect the current NRC employee badge characteristics.
3. Update DI-12.1, *Region III Security System Testing Process*, to describe the current requirement to review access permissions to the Region III server room and LAN closets (that are equipped with card readers) on a quarterly basis.
4. Update DI-NR-006, *Region III Switchboard Operations,* to reflect the current NRC employee badge characteristics and to describe functions now performed by the protective security officer instead of the receptionist.
5. Update RP-3.57, *System of Procedures, Notices, and Division Instructions*, to specify which regional procedures and divisional instructions require annual review and update.

[Page intentionally left blank]

Appendix. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The Region III information security risk evaluation objectives 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 III.
- Evaluate the effectiveness of agency security control techniques as implemented at Region III.

SCOPE

The scope of this information security risk evaluation included:

- The three floors Region III occupies at 2443 Warrenville Road, Suite 210, Lisle, Illinois 60532-4352.
- Region III seat-managed equipment.
- Region III NRC-managed equipment.

The information security risk 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 III in Lisle, IL, between August 6, 2012, and August 10, 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 the NRC IT security program, policies, and practices as implemented at Region III, and evaluated the effectiveness of agency security control techniques as implemented at Region III.

In conducting the information security risk evaluation, the following areas were reviewed: physical and environmental security controls, logical access controls, configuration management, IT security program, and continuity of operations and recovery. Specifically, the evaluation team conducted site surveys of the three floors Region III occupies at 2443 Warrenville Road, Suite 210, Lisle, Illinois 60532-4352, focusing on the areas that house IT equipment. The team conducted interviews with the Region III ISSO, the seat-management server administrator, the Region III server administrator, and other Region III staff members responsible for implementing the agency's IT security program at Region III. The evaluation team also conducted user interviews with 14 Region III employees, including two Resident Inspectors and one teleworker. The team reviewed documentation provided by Region III including floor plans, inventories of 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 III network and the Region III 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; and Joseph Rood, GWAPT, CISSP, CISA, from Richard S. Carson & Associates, Inc.