EVALUATION REPORT

Information Security Risk Evaluation of Region IV – Arlington, TX

OIG-13-A-07 December 20, 2012

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

OFFICE OF THE
INSPECTOR GENERAL

December 20, 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 IV – ARLINGTON, TX (OIG-13-A-07)

Attached is the Office of the Inspector General's (OIG) evaluation report titled, *Information Security Risk Evaluation of Region IV – Arlington, TX.*

The report presents the results of the subject evaluation. The agency agreed with the evaluation findings at the September 21, 2012, exit conference, and provided comments 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 415-5911.

Attachment: As stated

Information Security Risk Evaluation of Region IV – Arlington, TX

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

December 17, 2012

[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 IV office, which is located in Arlington, Texas.

OBJECTIVES

The Region IV 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 IV.
- Evaluate the effectiveness of agency security control techniques as implemented at Region IV.

RESULTS IN BRIEF

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

Continuity of Operations and Recovery

Backup procedures are inadequate. Specifically, backup procedures are not maintained and kept up-to-date and backups of NRC-managed servers are not sent to an offsite storage location. As a result, Region IV 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 do not have a current authority to operate. As a result, Region IV is not fully compliant with NRC requirements for laptop systems. The Region IV physical security plan is not 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 IV. A consolidated list of recommendations appears on page 11 of this report.

AGENCY COMMENTS

At an exit conference on September 21, 2012, agency officials agreed with the findings and provided comments which were incorporated, as appropriate, into this report. The agency opted not to submit formal comments.

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
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
PG	Policy Guide
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 IV office oversees regulatory activities in the western and southern midwestern United States; is located in Arlington, Texas; and operates under the direction of a Regional Administrator. The region covers a 22-State area, including 9 States with nuclear power plants, as well as the U.S. Pacific territories. Region IV also oversees the Grand Gulf Nuclear Station in Mississippi, which is located in Region II.

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 IV. A consolidated list of recommendations appears on page 11.

2 Objectives

The Region IV 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 IV.
- Evaluate the effectiveness of agency security control techniques as implemented at Region IV.

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

3 Findings

Region IV 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 IV 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 IV 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 IV IT security program are described in the following sections.

3.1 Continuity of Operations and Recovery

Region IV 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 IV has documented backup procedures for seat-managed servers and Region IV has developed a site-specific Occupant Emergency Plan.

However, the evaluation team found that backup procedures are inadequate. Specifically, backup procedures are not maintained and kept up-to-date and backups of NRC-managed servers are not sent to an offsite storage location. As a result, Region IV may not have reliable IT system backup information available if there is a need for system or file recovery.

3.1.1 Region IV Servers

Region IV 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 IV and include Web servers, application servers, and servers supporting the Region IV phone system. NRC-managed servers at Region IV are currently not included in any authorization boundary.

FINDING #1: Backup Procedures Are Inadequate

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 IV has not met all the requirements. Specifically, backup procedures are not maintained and kept up-to-date and backups of NRC-managed servers are not sent to an offsite storage location. As a result, Region IV may not have reliable IT system backup information available if there is a need for system or file recovery.

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.

NRC 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.

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

The Region IV seat-management contractor has developed backup procedures for seat-managed servers in Region IV. These procedures are documented in "Backup Procedures," last revised April 2, 2012. The seat-management contractor is only responsible for performing backups of seat-managed servers. While Region IV has developed and documented required backup procedures, the procedures do not reflect the server infrastructure currently in place in Region IV. For example, the backup procedures include a list of seat-managed servers covered by the document; however, this list includes two servers that are not found in the actual backup job run by the backup software. There are also two servers in the actual backup job that are not referenced in the documented backup procedures. The backup procedures also still include a reference to the previous seat-management contractor. The seat-management contract was transitioned to the current contractor in December 2011. In addition, the current seat-management contractor creates a Ghost[4] image of every server at least once a month, and whenever significant changes are made. However, procedures for creating Ghost images, including where those images are stored, are not documented.

NRC staff in Region IV is responsible for performing backups of NRC-managed servers. Data on NRC-managed servers is backed up to network attached storage. However, these procedures are not documented. In addition, backups of NRC-managed servers are not sent to an offsite storage location.

3.1.4 Potential Risk of Server Unavailability or Data Loss

While the backup procedures that are currently implemented should minimize data loss in the event of a computer failure, the procedures for the seat-managed servers are not up-to-date and

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

there are no procedures for the NRC-managed servers. 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 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. 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. As a result, Region IV 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:

1. Update the backup procedures for seat-managed servers to (i) reflect the current Region IV seat-managed server infrastructure; (ii) document current backup procedures for seat-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 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. Develop documented backup procedures for NRC-managed servers. The procedures should include the same level of detail as the backup procedures for seat-managed servers.
3. Develop and implement procedures for sending backups of NRC-managed servers to an offsite storage location in accordance with NRC requirements.

3.2 Information Technology Security Program

Overall, Region IV is following agency security policies and procedures regarding IT security. Region IV has developed regional policy guides that are generally up-to-date and are available on the Region IV internal Web site. Staff receive training regarding IT security during new employee orientation and receive a copy of the *Employee IT User Manual*, which includes a section on computer security, and the Information Systems Security Officer (ISSO) sends periodic cybersecurity reminders via e-mail on topics such as safe online shopping and phishing. Users are generally aware of and are following agency and Region IV IT security policies and procedures.

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

3.2.1 Region IV Laptop Systems

Laptops in use at Region IV are either seat-managed laptops or NRC-owned laptops. Seat-managed laptops in use at Region IV include those laptops that are part of the agency's new *working from anywhere/mobile desktop program*. NRC-owned laptops in use at Region IV

include loaner laptops, laptops in conference rooms and training rooms, and laptops used to process safeguards information (SGI).

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 IV include loaner laptops, laptops in conference rooms and training rooms, and laptops used to process SGI. However, the evaluation team found that some NRC-owned laptops do not have a current authority to operate (ATO). As a result, Region IV 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 IV has not established a general laptop system, which would include their loaner laptops and laptops found in conference rooms and training rooms. In addition, Region IV has one SGI laptop (and four standalone desktops) still on the NRC inventory of systems and a system called the Region IV SGI Automated Inventory System. The NRC inventory indicates five of these systems have an authorization to operate that expired in March 2009 and the Region IV SGI Automated Inventory System never had an authorization to operate. During the site visit to Region IV, the evaluation team was unable to determine whether any of the SGI systems on the NRC inventory were still in use and therefore should be covered under a Region IV SGI laptop system with a current ATO. Subsequent to the site visit, Region IV informed the evaluation team that SGI laptops and standalone desktops are no longer in use and are in the process of being decommissioned. Therefore, there is no need for Region IV to establish a Region IV SGI laptop system to cover these systems.

RECOMMENDATION

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

4. Establish a general laptop system and complete the process described in the *NRC Laptop Security Policy* for authorization of the general laptop system.

3.2.4 Regional Procedures and Instructions

Region IV uses regional office policy guides and notices to inform the staff of regional policies, procedures, and guidance, including those specific to the Region IV IT security program. Policy guides contain instructions, policies, procedures, or guidance intended to be of a permanent nature, remain in effect until they are revised or cancelled, and must be updated within 3 years of the date of issuance to ensure all information remains current. Regional notices contain information of a temporary nature and are intended to keep the staff informed, but do not establish comprehensive policy for the staff to follow. All notices contain an expiration date that does not exceed 6 months from the date of issuance. For both policy guides and notices, the originating division is responsible for ensuring their assigned documents are current.

The following are some examples of regional policy guides specific to the Region IV IT security program:

- Policy Guide (PG) 0754.2, *Physical Security Plan*, dated August 30, 2011 – describes the policies, procedures, and responsibilities for assuring protection of information, property and employees at Region IV.
- PG 0253-5, *Computer User's Guide*, dated April 19, 2012 – establishes guidelines for maintaining computer security and the general use of government computer resources in Region IV.
- PG 0759.3, *Region IV Security Program*, dated January 19, 2011 – establishes the overall structure and policy for all elements of the Region IV security programs.

FINDING #3: Region IV Physical Security Plan Is Not Up-to-Date

NRC has developed several security standards that specify the frequency of reviewing and updating IT security program procedures. However, the Region IV physical security plan is not 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

NRC 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 control 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. NRC 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.

PG 0001.11, *RIV Policy Guide and Office Notice System*, dated January 9, 2006, describes the system for initiating, revising, and deleting regional office policy guides and notices. PG 0001.11 requires policy guides to be updated within 3 years of the date of issuance to ensure all information remains current.

3.2.6 Agency Has Not Fully Met Requirements

Region IV has developed several regional policy guides specific to the Region IV IT security program. However, the evaluation team found that the Region IV physical security plan is not up-to-date. For example, several sections need to be updated to reflect the new office location. Region IV moved from 612 East Lamar Boulevard to 1600 East Lamar Boulevard in December 2011. The document also does not describe the current access control procedures for visitors. Some of the functions described in this document are now performed by the security guards[5] and a different form is used for visitor registration. This document is being updated and is currently under review with headquarters and Region IV executives. However, Region IV has not established a target completion date for the update.

PG 0001.11 requires policy guides to be updated within 3 years of the date of issuance to ensure all information remains current. 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 control 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.

[5] Region IV contracts through the Federal Protective Service for security guard services.

3.2.7 Impact on Region IV 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:

5. Update PG 0754.2, *Physical Security Plan*, to reflect the new office location, describe the current access control procedures for visitors, and describe functions now performed by the security guards.
6. Update PG 0001.11, *RIV Policy Guide and Office Notice System*, to specify which regional policy guides 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 the backup procedures for seat-managed servers to (i) reflect the current Region IV seat-managed server infrastructure; (ii) document current backup procedures for seat-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 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. Develop documented backup procedures for NRC-managed servers. The procedures should include the same level of detail as the backup procedures for seat-managed servers.
3. Develop and implement procedures for sending backups of NRC-managed servers to an offsite storage location in accordance with NRC requirements.
4. Establish a general laptop system and complete the process described in the *NRC Laptop Security Policy* for authorization of the general laptop system.
5. Update PG 0754.2, *Physical Security Plan*, to reflect the new office location, describe the current access control procedures for visitors, and describe functions now performed by the security guards.
6. Update PG 0001.11, *RIV Policy Guide and Office Notice System*, to specify which regional policy guides require annual review and update.

[Page intentionally left blank]

5 Agency Comments

At an exit conference on September 21, 2012, agency officials agreed with the findings and provided comments which were incorporated, as appropriate, into this report. The agency opted not to submit formal comments.

[Page intentionally left blank]

Appendix. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The Region IV 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 IV.
- Evaluate the effectiveness of agency security control techniques as implemented at Region IV.

SCOPE

The scope of this information security risk evaluation included:

- The four floors Region IV occupies at 1600 E. Lamar Boulevard, Arlington, Texas 76011-4511.
- Region IV seat-managed equipment.
- Region IV 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 IV in Arlington, TX, between September 17, 2012, and September 21, 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 IV, and evaluated the effectiveness of agency security control techniques as implemented at Region IV.

In conducting the information security risk evaluation, the following areas were reviewed: physical and environmental security controls, logical access controls, configuration management, continuity of operations and recovery, and IT security program. Specifically, the evaluation team conducted site surveys of the four floors Region IV occupies at 1600 E. Lamar Boulevard, Arlington, Texas 76011-4511, focusing on the areas that house IT equipment. The team conducted interviews with the Region IV ISSO, the seat-management server administrator, the Region IV server administrator, and other Region IV staff members responsible for implementing the agency's IT security program at Region IV. The evaluation team also conducted user interviews with 14 Region IV employees, including two Resident Inspectors and two teleworkers. The team reviewed documentation provided by Region IV 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 IV network and the Region IV 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 Diane Reilly, from Richard S. Carson & Associates, Inc.