EVALUATION REPORT

Information Security Risk Evaluation of Region I – King of Prussia, PA

OIG 13-A-06   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 I – KING OF PRUSSIA, PA (OIG-13-A-06)

Attached is the Office of the Inspector General's (OIG) evaluation report titled, *Information Security Risk Evaluation of Region I – King of Prussia, PA.*

The report presents the results of the subject evaluation. The agency agreed with the evaluation findings at the October 26, 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

Carson

Information Security Risk Evaluation of Region I – King of Prussia, PA

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

December 17, 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 I office, which is located in King of Prussia, Pennsylvania.

OBJECTIVES

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

RESULTS IN BRIEF

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

IT Security Program

Some NRC-owned laptops do not have a current authority to operate. As a result, Region I is not fully compliant with NRC requirements for laptop systems. 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 IT security program and implementation of FISMA at Region I. A consolidated list of recommendations appears on page 9 of this report.

AGENCY COMMENTS

At an exit conference on October 26, 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

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
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 I office oversees regulatory activities in the northeastern United States; is located in King of Prussia, Pennsylvania; and operates under the direction of a Regional Administrator. The region covers an 11-State area, including 8 States with nuclear power plants, as well as the District of Columbia. Region I also oversees all materials licensees 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 I. A consolidated list of recommendations appears on page 9.

2 Objectives

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

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

3 Findings

Region I 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 I 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 I automated and manual IT security controls are generally effective, some IT security controls need improvement. Specifics on the Region I IT security program are described in the following section.

3.1 Information Technology Security Program

Overall, Region I is following agency security policies and procedures regarding IT security. Region I has developed regional implementing instructions that are generally up-to-date and are available on the Region I internal Web site. Staff receive training regarding IT security during new employee orientation, the Information Systems Security Officer (ISSO) sends periodic cybersecurity reminders via e-mail on topics such as locking your workstation and phishing, the ISSO maintains a SharePoint portal containing announcements on various cybersecurity topics, and there is a Web page for Region I "How-To" instructions. Users are generally aware of and are following agency and Region I IT security policies and procedures.

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

3.1.1 Region I Laptop Systems

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

FINDING #1: 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 I include a pool of loaner laptops, laptops in conference rooms, 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 I is not fully compliant with NRC requirements for laptop systems.

3.1.2 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.

3.1.3 Agency Has Not Fully Met Requirements

Region I has not established a general laptop system, which would include their pool of loaner laptops and laptops found in conference rooms. However, the Region I laptop pool is in the process of being decommissioned, with all loaner laptops and laptops in the conference rooms to be replaced with *mobile desktops*. Therefore, there is no need for Region I to establish a Region I general laptop system to cover these systems.

In addition, Region I has 20 SGI laptops, 7 standalone desktops, and 8 “sensitive” hard drives still on the NRC inventory of systems as well as a system called the Region I SGI Automated Inventory System, which may include the laptops, standalone desktops, and sensitive hard drives. The NRC inventory indicates some of these laptops, standalone desktops, and sensitive hard drives, have authorizations to operate that expired in early 2009, while some never had an authorization to operate. The NRC inventory also indicates the Region I SGI Automated Inventory System never had an authorization to operate. Region I is in the process of decommissioning all laptops, standalone desktops, and sensitive hard drives used to process SGI. Therefore, there is no need for Region I to establish a Region I SGI laptop system to cover these systems.

3.1.4 Regional Procedures and Instructions

Region I uses regional implementing instructions when (i) agency policy requires a regional implementing instruction, (ii) clarification is required to help staff understand the agency policy or guidance document, (iii) regional management establishes expectations beyond those in the agency policy or guidance document and specific guidance is required to assure consistent implementation, or (iv) there is no specific agency policy or guidance on an issue that regional management concludes requires a regional policy or implementing instruction to assure consistent implementation. Regional implementing instructions include regional instructions and divisional instructions, directives, and policies, which establish requirements and expectations, and therefore have strict controls for review and maintenance. Regional implementing instructions also include regional "How-To" instructions and standard operating procedures, which are informational in nature and therefore do not require the same level of review and maintenance. Regional instructions and divisional instructions, directives, and policies must be reviewed at least every 3 years and "How-To" instructions and standard operating procedures must be reviewed periodically by the responsible organization to determine if changes are necessary.

The following are some examples of regional implementing instructions specific to the Region I IT security program:

- Region I Instruction 0710.1, *Region I Security Plan*, Revision 9, dated March 21, 2006 – establishes policies, procedures, and responsibilities for assuring protection of personnel, information, and property.
- Region I Instruction 0730.1, *NRC Identification Badge Issuance and Protection*, Revision 4, dated August 7, 2005 – provides guidance concerning issuance of badges to regional personnel.

FINDING #2: 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, regional implementing instructions specific to the Region I 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.

3.1.5 Requirements for Updating Procedures

NRC Computer Security Office Standard (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, *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.

Regional Instruction 0180.1, *Region I System of Instructions*, Revision 6, dated October 15, 2012, establishes the process and requirements for developing and maintaining regional implementing instructions. Regional instruction 0180.1 requires regional instructions and divisional instructions, directives and policies to be reviewed at least every 3 years and "How-To" instructions and standard operating procedures to be reviewed periodically by the responsible organization to determine if changes are necessary.

3.1.6 Agency Has Not Fully Met Requirements

Region I has developed several regional implementing instructions specific to the Region I IT security program. However, the evaluation team found that the following regional implementing instructions are not up-to-date.

- Region I Instruction 0710.1, *Region I Security Plan* – several sections need to be updated to reflect access controls at the new office location. Region I moved from 475 Allendale Road to 2100 Renaissance Boulevard in May 2012. The document also does not describe the current access control procedures for visitors. For example, a different form is used for visitor registration and some of the functions described in this document are now performed by the protective security officer[4] (e.g., issuing temporary badges, ensuring all issued badges are returned, and ensuring visitors are logged in/out) and not the receptionist.
- Region I Instruction 0730.1, *NRC Identification Badge Issuance and Protection* – this document does not describe the current badge issuance procedures and references old badge categories that are no longer in use at the agency.

Region I is in the process of updating Region I Instruction 0710.1, *Region I Security Plan*, with a target completion date of November 30, 2012. Region I is in the process of determining whether the target completion date needs to be extended due to a change in focus for the document. Region I has issued an interim document, *Security Access to Region I Office*, which describes the current access controls in place for both NRC employees and visitors, but not to the level of detail found in Region I Instruction 0710.1.

Regional Instruction 0180.1, *Region I System of Instructions*, requires regional instructions to be reviewed at least every 3 years by the responsible organization to determine if changes are necessary. 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.

3.1.7 Impact on Region I 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.

[4] Region I contracts through the Federal Protective Service for security guard services.

RECOMMENDATIONS

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

1. Update Region I Instruction 0710.1, *Region I 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.
2. Update Region I Instruction 0730.1, *NRC Identification Badge Issuance and Protection*, to describe the current badge issuance procedures and to reflect the current NRC employee badge characteristics.
3. Update Regional Instruction 0180.1, *Region I System of Instructions*, to specify which regional implementing 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 Region I Instruction 0710.1, *Region I 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.
2. Update Region I Instruction 0730.1, *NRC Identification Badge Issuance and Protection*, to describe the current badge issuance procedures and to reflect the current NRC employee badge characteristics.
3. Update Regional Instruction 0180.1, *Region I System of Instructions*, to specify which regional implementing instructions require annual review and update.

[Page intentionally left blank]

5 Agency Comments

At an exit conference on October 26, 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 Region I 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 I.
- Evaluate the effectiveness of agency security control techniques as implemented at Region I.

SCOPE

The scope of this information security risk evaluation included:

- The three floors Region I occupies at 2100 Renaissance Boulevard, King of Prussia, Pennsylvania 19406-2713.
- Region I seat-managed equipment.
- Region I 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 I in King of Prussia, PA, between October 22, 2012, and October 26, 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 I, and evaluated the effectiveness of agency security control techniques as implemented at Region I.

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 three floors Region I occupies at 2100 Renaissance Boulevard, King of Prussia, Pennsylvania 19406-2713, focusing on the areas that house IT equipment. The team conducted interviews with the Region I ISSO, the seat-management server administrator, the Region I server administrator, and other Region I staff members responsible for implementing the agency's IT security program at Region I. The evaluation team also conducted user interviews with 16 Region I employees, including 3 Resident Inspectors and 4 teleworkers. The team reviewed documentation provided by Region I 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 I network and the Region I 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.