EVALUATION REPORT

Information Security Risk Evaluation of
NRC's Technical Training Center – Chattanooga, TN

OIG 13-A-11 January 30, 2013

Information Security Risk Evaluation of
NRC's Technical Training Center – Chattanooga, TN

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

January 22, 2013

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

OFFICE OF THE
INSPECTOR GENERAL

January 30, 2013

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 NRC's TECHNICAL TRAINING CENTER – CHATTANOOGA, TN (OIG-13-A-11)

Attached is the Office of the Inspector General's (OIG) evaluation report titled *Information Security Risk Evaluation of NRC's Technical Training Center –Chattanooga, TN.*

The report presents the results of the subject evaluation. The agency agreed with the evaluation findings at the December 7, 2012, exit conference and did not provide any changes to the draft report.

Please provide information on actions taken or planned on the recommendation 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

[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 (TTC). This report presents the results of the information security risk evaluation for the TTC, which is located in Chattanooga, Tennessee.

OBJECTIVES

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

RESULTS IN BRIEF

The TTC 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, TTC 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, the TTC is not fully compliant with NRC requirements for laptop systems.

RECOMMENDATIONS

This report makes a recommendation to the Executive Director for Operations to improve NRC's IT security program and implementation of FISMA at the TTC.

AGENCY COMMENTS

At an exit conference on December 7, 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]

ABBREVIATIONS AND ACRONYMS

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
TTC	Technical Training Center

[Page intentionally left blank]

TABLE OF CONTENTS

[Page intentionally left blank]

1 Background

The U.S. Nuclear Regulatory Commission (NRC) Technical Training Center (TTC) provides training for the staff in various technical disciplines associated with the regulation of nuclear materials and facilities and is located in Chattanooga, Tennessee. The TTC is part of the Office of the Chief Human Capital Officer and operates under the direction of the Associate Director for Human Resources Training and Development.

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.

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 TTC to evaluate IT security programs in place at those locations, to include an assessment of potential

[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…."

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 the TTC.

2 Objectives

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

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

3 Findings

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

3.1 Information Technology Security Program

Overall, the TTC is following agency security policies and procedures regarding IT security. The TTC has developed operating procedures that are generally up-to-date and are available on the Human Resources Training and Development internal Web site. Staff receive training regarding IT security during new employee orientation, take annual security awareness training, and the Information Systems Security Officer (ISSO) sends periodic e-mails related to IT

security. Users are generally aware of and are following agency and TTC IT security policies and procedures.

However, the evaluation team found issues with the TTC laptop systems.

3.1.1 TTC Laptop Systems

Laptops in use at the TTC are either seat-managed laptops or NRC-owned laptops. Seat-managed laptops in use at the TTC include one laptop that is part of the agency's new *work from anywhere/mobile desktop program*. NRC-owned laptops in use at the TTC include a pool of laptops used for various purposes and one laptop used to process safeguards information (SGI).

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 the TTC include a pool of laptops used for various purposes and one laptop used to process SGI. However, the evaluation team found that some NRC-owned laptops do not have a current authority to operate. As a result, the TTC 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

The TTC has not established a general laptop system to cover their pool of laptops; however, the TTC laptop pool is in the process of being authorized to operate. A system description has been written for the TTC general laptop system and the laptops have been evaluated using security criteria provided by the Computer Security Office. The TTC plans to submit a request for authority to operate the general laptop system in the next few months.

In addition, the TTC has one laptop used to process SGI, for which the TTC developed a physical security plan for the protection of safeguards information, dated January 2009. However, the TTC has not established a TTC SGI laptop system to cover this laptop, and the physical security plan does not meet the requirements for a system description of an SGI laptop system. For example, the document does not list those responsible for the SGI laptop, such as the system owner, ISSO, and system administrator, and does not include the required laptop specifics such as encryption, hardware, installed software, and any deviations from the standard SGI laptop security plan. In addition, the SGI laptop has not been officially authorized to operate.

RECOMMENDATION

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

1. Establish an SGI laptop system and complete the process described in the *NRC Laptop Security Policy* for authorization of the SGI laptop system.

4 Agency Comments

At an exit conference on December 7, 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 TTC 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 the TTC.
- Evaluate the effectiveness of agency security control techniques as implemented at the TTC.

SCOPE

The scope of this information security risk evaluation included:

- The four floors the TTC occupies at 5746 Marlin Road, Chattanooga, Tennessee 37411-5677.
- TTC seat-managed equipment.
- TTC 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 the TTC in Chattanooga, TN, between December 3, 2012, and December 7, 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 the TTC, and evaluated the effectiveness of agency security control techniques as implemented at the TTC.

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 the TTC occupies at 5746 Marlin Road, Chattanooga, Tennessee 37411-5677, focusing on the areas that house IT equipment. The team conducted interviews with the TTC alternate ISSO, the seat-management server administrator, the TTC server administrator, and other TTC staff members responsible for implementing the agency's IT security program at the TTC. The evaluation team also conducted user interviews with 12 TTC employees. The team reviewed documentation provided by the TTC 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 TTC network. The scan did not include the network that supports the simulators.

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 Virgil Isola, CISSP, from Richard S. Carson & Associates, Inc.