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

OFFICE OF THE
INSPECTOR GENERAL

August 17, 2017

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017 – TECHNICAL TRAINING CENTER, CHATTANOOGA, TN (OIG-17-A-22)

The Office of the Inspector General (OIG) conducted an independent evaluation of NRC's implementation of the *Federal Information Security Modernization Act of 2014 (FISMA 2014) for Fiscal Year (FY) 2017* at the Technical Training Center (TTC) located in Chattanooga, TN. OIG found that the TTC information technology (IT) security program, including TTC IT security policies, procedures, and practices, is generally effective. However, the TTC System Hardware and Software Inventory is incomplete and agency-managed laptops and standalone desktops are not authorized to operate in accordance with NRC policies, procedures, and processes. OIG makes recommendations to address these findings.

Additionally, OIG identified an issue with unclear and out-of-state laptop security policies and procedures that will be further evaluated during the FY 2017 FISMA evaluation.

BACKGROUND

The U.S. Nuclear Regulatory Commission (NRC) TTC provides training for the staff in various technical disciplines associated with the regulation of nuclear materials and facilities and is located in Chattanooga, TN. 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.

On December 18, 2014, the President signed FISMA 2014, reforming the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[1] 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 the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General or by an independent external auditor.[2]

NRC OIG retained Richard S. Carson & Associates, Inc., to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017 at NRC's four regional offices and the TTC. This report presents the results of the independent evaluation at the TTC.

[1] 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 2014, the agency uses the term "information technology security program."

[2] While FISMA 2014 uses the language "independent external auditor," Office of Management and Budget 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…."

OBJECTIVE

The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017 at the TTC and to evaluate the effectiveness of agency information security policies, procedures, and practices as implemented at this location.

RESULTS

The TTC IT security program, including TTC IT security policies, procedures, and practices, is generally effective. However, the TTC System Hardware and Software Inventory is incomplete and agency-managed laptops and standalone desktops are not authorized to operate in accordance with NRC policies, procedures, and processes.

TTC System Hardware and Software Inventory Is Incomplete

Federal guidance requires organizations to develop and document an inventory of information system components. NRC has defined the specific information to be captured in the inventory and requires the inventory to be reviewed and updated at least annually and within 30 days of hardware or software changes within a system. However, the TTC System Hardware and Software Inventory is incomplete. As a result, configuration management and continuous monitoring activities may not be effective.

What Is Required

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to develop

and document an inventory of information system components. Information Security Directorate (ISD) standard ISD-STD-0020, *Organization-Defined Values for System Security and Privacy Controls*, defines the specific information to be captured in the inventory and requires the inventory to be reviewed and updated at least annually and within 30 days of hardware or software changes within the system. ISD process ISD-PROS-2102, *System Cybersecurity Assessment Process*, provides additional details on the specific information to be captured in the inventory, and requires an accurate, complete, and up-to-date inventory for all system cybersecurity assessment activities.

What We Found

The TTC System consists of five separate subsystems, including Web applications, external guest network, innovation network, private branch exchange, and simulation network. The TTC System's inventory of components is documented in the TTC System Hardware and Software Inventory. Inventory information is also captured in the TTC's local property management system. However, the TTC Hardware and Software Inventory does not include simulation network components. A simulator upgrade project was completed in late 2016/early 2017; however, the TTC Hardware and Software Inventory has not been updated to include the new components. This document is currently in the process of being updated as part of the TTC System's periodic system cybersecurity assessment, but the simulation network components have not been included in the update. Subsequent to the completion of fieldwork, TTC stated data for the inventory has been gathered and will be included in the updated document.

Why This Occurred

As stated in the TTC Simulation Network system security plan, "the number of simulator network components is quite large and since they were never physically assessed they were never added to the TTC Hardware and Software Inventory document." The security plan further

stated the inventory would be updated as soon as the simulator upgrade projects were completed.

Why This Is Important

A complete component inventory is necessary for effective configuration management as well as for information security continuous monitoring. ISD-PROS-2102 requires an accurate, complete, and up-to-date inventory for all system cybersecurity assessment activities in support of continuous monitoring.

RECOMMENDATION

OIG recommends that the Executive Director for Operations

1. Update the TTC System Hardware and Software Inventory to include all individual simulation network components.

Agency-Managed Laptops and Standalone Desktops Are Not Authorized to Operate

NRC has developed several policies, procedures, configuration guidance, and configuration standards regarding agency-managed laptops and standalone desktops. All NRC laptops and standalone desktops must belong to a system boundary and that system must be authorized to operate. However, TTC has a number of agency-managed laptops and standalone desktops that are not authorized to operate. One laptop has an authorization to operate (ATO) that has lapsed, and the remaining laptops and standalone desktops were never issued an ATO. As a result, these laptops and standalone desktops may not have adequate security controls in place.

What Is Required

Management Directive and Handbook 12.5, *NRC Cybersecurity Program*, require all assets that process, store, or transmit NRC information for or on behalf of NRC to be a part of a system that is identified in the IT system inventory. The ISD Web page on Authorization and Continuous Monitoring states that all computing components (i.e., all hardware and software) must be defined within a system boundary.

Each year, the NRC Executive Director for Operations issues a memorandum and instructions requiring system owners to perform cybersecurity risk management activities required for FISMA. The FY 2017 memorandum states all NRC laptops and standalone desktops must belong to a system boundary (which may contain one or more devices) and that system must be authorized to operate. The memorandum also describes three types of laptop/standalone desktop systems that can be used to authorize such components.

In April 2009, NRC issued a *Laptop Security Policy* that applies to all NRC laptops owned, managed, and/or operated by NRC or by other parties on behalf of NRC. This would include agency-managed laptops at TTC. All agency-managed laptops should be included in one of the three types of laptop/standalone desktops defined in the policy. This policy no longer appears on the ISD Cybersecurity Policy Web page.

In conjunction with the *Laptop Security Policy*, NRC also developed general laptop configuration guidance, a standard System Security Plan for each type of laptop system, configuration standards, and minimum security checklists. The majority of these documents have not been updated since 2011.

What We Found

Agency-managed laptops and standalone desktops are not authorized to operate. One laptop has an ATO that has lapsed, and the remaining laptops and standalone desktops were never issued an ATO.

TTC Laptop Has a Lapsed ATO

TTC has a laptop that is used once a year in support of three TTC courses to display videos and presentations containing safeguards information (SGI). This laptop was issued an ATO on January 28, 2014. The authorization memorandum states the authorization is in effect as long as security controls specified in the security plan are implemented and operated as intended, and independent annual security control and vulnerability testing are conducted. However, some security controls specified in the security plan are not being performed, such as monthly reviews of authorized users and periodic reviews of laptop audit logs. In addition, annual security control and vulnerability testing were not conducted. Therefore, the authorization for this laptop has lapsed and is no longer in effect. TTC is planning on decommissioning this laptop and will transition to the Safeguards Local Area Network and Electronic Safe (SLES) thin client for presenting SGI training at the TTC.

TTC Laptops and Standalone Desktops Were Never Issued an ATO

TTC also has approximately 80 additional laptops and standalone desktops that are used for a variety of functions. The majority are used by students attending TTC courses. These laptops connect to the innovation network and download course content as part of TTC's paperless classroom initiative. Additional laptops and standalone desktops are used to perform management and support functions for the various TTC System subsystems, such as system administration, troubleshooting, and vulnerability scanning. Others are used for testing new software or for demonstrating the impacts of viruses and malicious software. None of these laptops and standalone desktops are connected to the NRC's production network – they are only used to connect to TTC System subsystems. TTC does apply patches and keeps antivirus definitions up-to-date on these laptops. However, these laptops and standalone desktops are not part of the TTC System boundary, have not had any type of system cybersecurity assessment, and are not formally authorized to operate.

Why This Occurred

During the initial authorization system cybersecurity assessment of the TTC System in 2013, TTC was told by the assessment team that the laptops and standalone desktops had to have their own authorization to operate and could not be part of the TTC System boundary. However, Management Directive and Handbook 12.5, *NRC Cybersecurity Program*, and the FY 2017 risk management activities memorandum and instructions are unclear as to whether agency-managed laptops and standalone desktops must have a separate authorization to operate or can be incorporated into the existing TTC System boundary. All other NRC policies and procedures regarding agency-managed laptops and standalone desktops are inconsistent and out-of-date. The issue with the unclear and out-of-date laptop security policies and procedures will be evaluated further during the NRC's FY 2017 FISMA independent evaluation.

Why This Is Important

Although none of the agency-managed laptops and standalone desktops are connected to the NRC's production network, they may be connected to the Internet to get software updates or to browse the Internet. TTC does apply patches and keeps anti-virus definitions up-to-date on these laptops. However, they have not had any type of system cybersecurity assessment performed to determine if security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements. In addition, annual security control and vulnerability testing were not conducted on these laptops. Inadequate security controls could result in inadvertent release of sensitive NRC information if an agency-managed laptop or standalone workstation is connected to the Internet, or could result in the introduction of malicious software back into the TTC System environment.

RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

2. Re-authorize the SGI laptop or find an alternate solution for presenting SGI materials in the classroom.

3. Add the agency-managed laptops and standalone desktops to the TTC System boundary and perform all required system cybersecurity assessment processes and procedures.

AGENCY COMMENTS

An exit conference was held with the agency on June 23, 2017. After this meeting, a discussion draft was provided to the agency for their comment. Agency management stated their general agreement with the results and opted not to provide formal comments for inclusion in this report.

SCOPE AND METHODOLOGY

Scope

The scope of this evaluation included the following:

- The four floors the TTC occupies at 5746 Marlin Road, Chattanooga, TN 37411-5677.
- TTC seat-managed IT components[3] and agency-managed IT components.
- National security systems (including systems processing safeguards information) housed at the TTC.

The evaluation work was conducted during a site visit to the TTC in Chattanooga, TN, between June 19, 2017, and June 23, 2017. Any information received from NRC subsequent to the completion of fieldwork was incorporated when possible. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, evaluators considered the possibility of fraud, waste, or abuse in the program.

Methodology

The evaluation assessed the following focus areas: inventory of systems, the NRC Risk Management Framework and Authorization Process for systems, logical access controls and privileged access, contingency planning, configuration management, and IT security architecture. The evaluation team conducted a site survey of one room housing national security systems (including systems processing safeguards information).

The team reviewed documentation provided by the TTC including floor plans; inventories of IT systems, hardware and software; local policies and procedures; security plans; operations guides and standard operating

[3] Seat-managed components provide core IT services at TTC, and include security appliances, routers, switches, servers (e.g., domain controllers, mail servers, file servers, multi-purpose servers, print servers), desktops, laptops, and printers. They are managed by NRC's seat-management contractor and are included in the authorization boundary of the IT Infrastructure system.

procedures; contingency plans and business impact assessments; configuration management plans; and the Occupancy Emergency Plan.

The team conducted interviews with the TTC System Information Systems Security Officer, server administrators, and other TTC employees responsible for implementing the NRC IT security program at the TTC. The evaluation team also conducted interviews with 15 TTC employees, including 3 teleworkers.

The information security risk evaluation also included a network vulnerability assessment scan of the TTC network. The evaluation team immediately notified the TTC of any critical vulnerabilities that were found. Subsequent to the completion of fieldwork, the TTC was provided with full details on all of the vulnerabilities identified by the scan.

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

- NIST standards and guidelines.
- Council of the Inspectors General on Integrity & Efficiency, *Quality Standards for Inspection and Evaluation*, January 2012.
- Management Directive and Handbook 12.5, *NRC Cybersecurity Program*.
- NRC Information Security Directorate policies, processes, procedures, standards, and guidelines.
- NRC OIG guidance.

The evaluation was conducted by Jane M. Laroussi, CISSP, and Maya Tyler, from Richard S. Carson & Associates, Inc.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TDD 7-1-1, or 1-800-201-7165

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.