MEMORANDUM

DATE: January 24, 2025

TO: Mirela Gavrilas
Executive Director for Operations

FROM: Hruta Virkar, CPA ***/RA/***
Assistant Inspector General for Audits & Evaluations

SUBJECT: PERFORMANCE AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2024 TECHNICAL TRAINING CENTER: CHATTANOOGA, TENNESSEE (OIG-NRC-25-A-04)

The Office of the Inspector General (OIG) contracted with Sikich CPA LLC (Sikich) to conduct the *Performance Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024 Technical Training Center: Chattanooga, Tennessee*. Attached is Sikich's final report on the audit. The objective was to assess the effectiveness of the information security policies, procedures, and practices of the U.S. Nuclear Regulatory Commission's (NRC) Technical Training Center (TTC). The findings and conclusions presented in this report are the responsibility of Sikich. The OIG's responsibility is to provide oversight of the contractor's work in accordance with generally accepted government auditing standards.

The report presents the results of the subject performance audit. The agency's staff indicated that they had no formal comments for inclusion in this report.

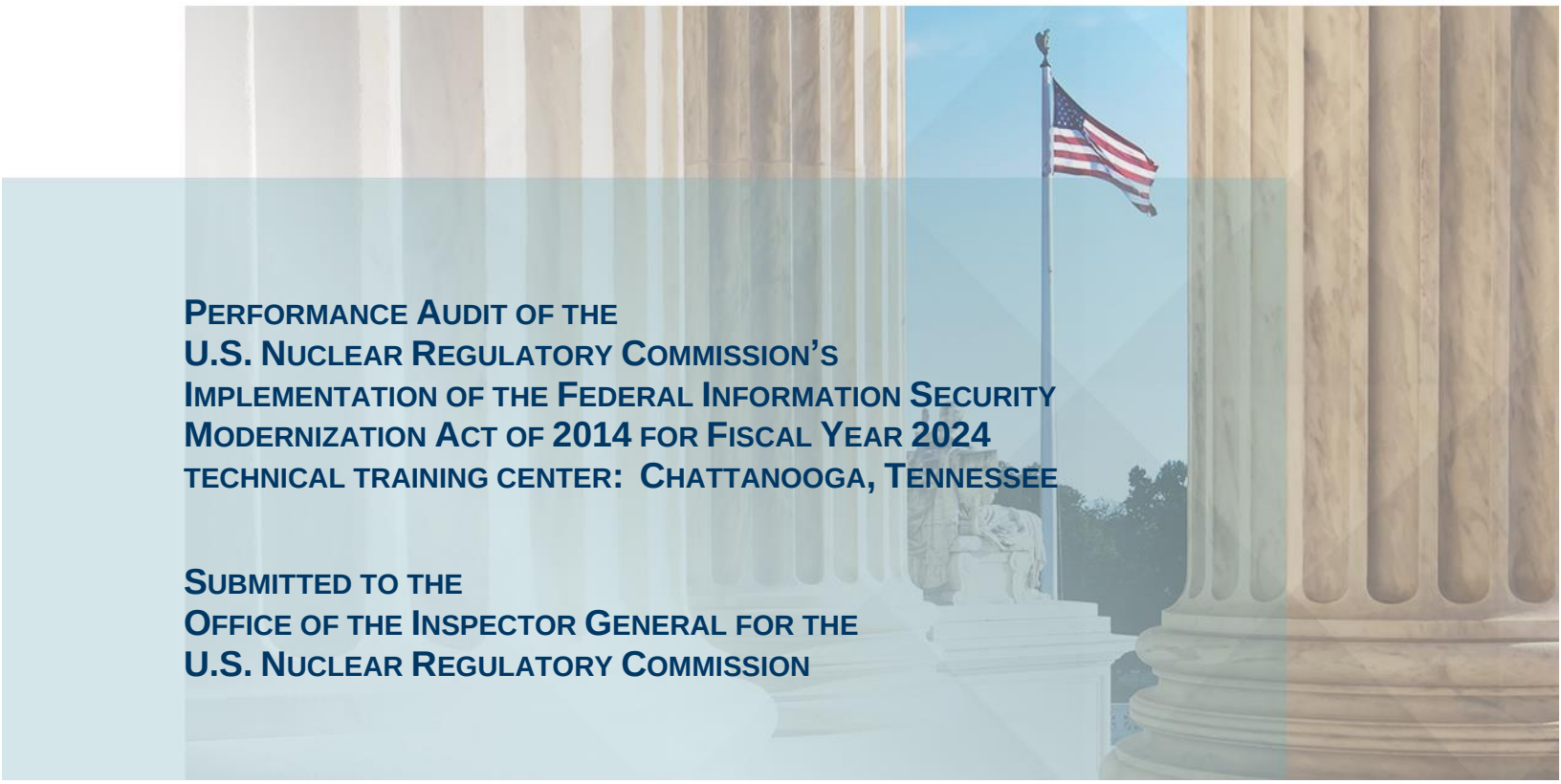
For the period March 2024 through October 2024, Sikich found that although the NRC generally implemented effective information security policies, procedures, and practices for the TTC, the agency's implementation of a subset of selected controls was not fully effective. There were weaknesses in the TTC's information security program and practices, and as a result, six recommendations were made to assist the TTC in strengthening its information security program.

Please provide information on actions taken or planned on each of the recommendations within 30 calendar days of the date of this report. Actions taken or planned are subject to OIG follow-up 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 301.415.1982 or Mike Blair, Team Leader, at 301.415.8399.

Attachment:
As stated

cc: J. Martin, ADO
S. Miotla, DADO
J. Jolicoeur, OEDO
OIG Liaison Resource
EDO_ACS Distribution

SIKICH®



PERFORMANCE AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2024 TECHNICAL TRAINING CENTER: CHATTANOOGA, TENNESSEE

SUBMITTED TO THE OFFICE OF THE INSPECTOR GENERAL FOR THE U.S. NUCLEAR REGULATORY COMMISSION

PERFORMANCE AUDIT REPORT

JANUARY 24, 2025

ACCOUNTING TECHNOLOGY ADVISORY

SIKICH®

333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

SIKICH.COM

January 24, 2025

The Honorable Robert J. Feitel
Inspector General
U.S. Nuclear Regulatory Commission

Dear Mr. Feitel:

Sikich CPA LLC (Sikich)[1] is pleased to submit the attached report detailing the results of our performance audit of the U.S. Nuclear Regulatory Commission's (NRC) Technical Training Center's (TTC) information security program and practices for Fiscal Year (FY) 2024 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires federal agencies, including the NRC, to perform an annual independent evaluation of their information security programs and practices. FISMA states that the evaluation is to be performed by the agency Inspector General (IG) or by an independent external auditor as determined by the IG. The NRC Office of the Inspector General (OIG) engaged Sikich to conduct this performance audit.

The NRC OIG requested that Sikich include two of the NRC's four regional offices and the NRC's TTC in its independent evaluation of the NRC's implementation of FISMA for FY 2024. This report presents the audit results for the NRC's TTC. We conducted the audit fieldwork remotely from Alexandria, Virginia, and onsite at the TTC facility in Chattanooga, Tennessee, from March through October 2024.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, as issued by the Comptroller General of the United States. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We describe our objective, scope, and methodology in **Appendix B: Objective, Scope, and Methodology**.

We appreciate the assistance that NRC management and staff provided.

Sikich CPA LLC
Alexandria, VA

[1] Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's (CLA's) federal practice, including its work for the NRC.

TABLE OF CONTENTS

I. Executive Summary

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also requires agency Inspectors General to assess the effectiveness of their agency's information security program and practices. The Office of Management and Budget and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish baseline security requirements for agencies.

The U.S. Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) engaged Sikich CPA LLC (Sikich) to conduct a performance audit to assess the effectiveness of the NRC's Technical Training Center's (TTC) information security policies, procedures, and practices.[2] The TTC is located in Chattanooga, Tennessee, although organizationally the TTC is within the NRC's Office of the Chief Human Capital Officer (OCHCO), which otherwise operates out of the NRC's headquarters in Rockville, Maryland. The TTC provides training for the NRC staff in various technical disciplines associated with the regulation of nuclear materials and facilities.[3]

The audit included an assessment of the NRC's TTC's implementation of select security controls[4] from NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. We conducted the audit fieldwork remotely from Alexandria, Virginia, and onsite at the TTC facility in Chattanooga, Tennessee from March 2024 through October 2024.

II. Summary of Results

We concluded that the NRC's information security policies, procedures, and practices are generally effective as they relate to the TTC. For example, the NRC:

- Maintained effective onboarding processes for new hires at the TTC.
- Implemented effective inventory practices for high and low-value TTC assets.
- Conducted a contingency plan exercise for the TTC system.[5]

Although we concluded that the NRC generally implemented effective information security policies, procedures, and practices for the TTC, the agency's implementation of a subset of selected controls was not fully effective. We noted weaknesses related to the employee separation process, issuing an updated Authority to Operate (ATO)[6] for the TTC system, and

[2] The NRC OIG requested that Sikich include two of the NRC's four regional offices and the TTC in the independent evaluation of the NRC's implementation of FISMA for Fiscal Year (FY) 2024.
[3] https://www.nrc.gov/about-nrc/locations.html
[4] The security controls selected for testing are listed in Appendix B: Objective, Scope, and Methodology.
[5] The TTC's primary function is to provide technical training to NRC personnel in a classroom setting using simulated scenarios. The simulations are conducted using a simulation network (SimNet) that is isolated from all other networks and systems.
[6] NIST defines an ATO as the official management decision issued by a designated accrediting authority (DAA) or principal accrediting authority (PAA) to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. ATO - Glossary | CSRC

physical access controls. As a result, we made six recommendations to assist either the NRC or the TTC specifically in strengthening its information security program.

The following section provides detailed information regarding each finding. **Appendix A** provides background information, **Appendix B** describes the audit objective, scope, and methodology, and **Appendix C** includes management's response.

III. AUDIT RESULTS

Finding 1: The NRC Should Improve Its Separation Processes

The NRC did not disable the Active Directory accounts of separated TTC employees in a timely manner. Specifically, for the 2 TTC employees separated between October 1, 2023, and July 18, 2024, the NRC disabled the Active Directory accounts at 13 and 24 days respectively after the employee's effective separation date.

The Office of the Chief Information Officer (OCIO) management indicated that the employee separation process has several dependencies that rely on OCIO, the Office of the Chief Human Capital Officer (OCHCO), and the Office of Administration (ADM). As currently designed, the separation process does not always remove access for separated employees in a timely manner. Management's review of these accounts showed that the Enterprise Identify Hub (EIH) automation correctly disabled accounts on the same day the NRC terminated the employee's access authorizations in the Personnel Security Adjudication Tracking System (PSATS). However, the Personnel Security Branch takes action in PSATS based on a file it receives from OCHCO titled "Employee Separations for the Last 28 Days." OCHCO sends this file to the Personnel Security Branch once every two weeks, and the Personnel Security Branch generally takes action within one to two weeks.

OCIO management stated that it will coordinate with OCHCO and ADM to review the business processes and identify any opportunities for shortening these timelines. Additionally, OCIO will review the organizationally defined value for account disablements to ensure that this value is reasonable and consistent with operational realities and acceptable risk levels.

The NRC OCIO Computer Security Standard (CSO-STD-0020), *System Security and Privacy Controls Standard*, dated December 8, 2023, specifies the following:

- Personnel Security (PS-4), *Personnel Termination*, requires that system access be disabled within a time period no later than the last day of employment/contract for voluntary termination and no later than user notification for involuntary termination.
- Access Control (AC-2), Enhancement 3, *Account Management: Disable Accounts*, requires that accounts be disabled within 24 hours when they are no longer associated with a user or individual.

If the NRC does not disable separated employees' accounts in a timely manner, it increases the risk of unauthorized access to NRC information systems and data.

Recommendation 1: We recommend that the NRC OCIO management, in coordination with OCHCO and ADM, evaluate the NRC's separation policies and procedures and re-engineer the related business processes and the automation used to disable separated employees' accounts to ensure that the NRC terminates these accounts in a timely manner.

Finding 2: The NRC Should Update the ATO for the TTC System to Reflect the Current Operating Environment

The NRC's ATO, for the TTC system[7] dated September 4, 2013, did not reflect the current system environment and referenced outdated systems. Specifically, the ATO memorandum noted that the TTC houses several miscellaneous web-based applications that are used for training and support purposes. However, the web-based applications are no longer part of the TTC system environment, and the ATO memorandum was not updated to reflect the changes to the environment.

The NRC maintained an ongoing authorization for the TTC system, where periodic system control assessments were conducted to maintain the ongoing authorization. However, this review did not evaluate the original decision and update the system boundaries within the ATO memorandum, as necessary.

The NRC OCIO Computer Security Standard (CSO-STD-0020), *System Security and Privacy Controls Standard*, dated December 8, 2023, specifies the following:

- Assessment, Authorization, and Monitoring (CA-6), *Authorization*, requires that the NRC updates the authorization in accordance with Authorization Official (AO) determined frequencies and conditions for the systems (e.g., at least every 3 years, ongoing).

By not maintaining an up-to-date ATO memorandum, the AO may not be aware of all components of the system and the risks associated with system.

Recommendation 2: We recommend that TTC and NRC management evaluate the TTC system ATO memorandum for revision and update it to reflect the current operating environment.

Finding 3: The NRC Should Improve Physical Access Controls at the TTC

We identified the following issues related to physical access controls for the NRC's TTC facility:

- **Network Equipment Access** – The TTC maintained an NRC Information Technology Infrastructure Patch Panel[8] for the second floor, which was not secured and was accessible by members in a simulation training class. Additional securities were put into place to restrict access to the simulation room through two-factor authentication; however, the room is regularly utilized for simulation training by trainees that may not be on the two-factor authentication listing.[9]

  Management indicated that this was an NRC OCIO decision at the time of implementation and that the TTC is working with OCIO to install a cage.

- **Emergency Shutoff Access** - 3 of the 6 Simulation Training Rooms had uncovered emergency shutoff switches, which risked accidental or malicious activation. The TTC had

[7] This ATO covers the simulation network (SimNet) system environment.
[8] Networking equipment for the second floor of the NRC's TTC facility, which includes ethernet connection points and unobstructed universal serial bus ports to the equipment.
[9] Two factor authentication for the TTC simulation room had been configured for the TTC employees and instructors. The access control does not include trainees, such as NRC inspectors, member state visitors, or other federal agencies employees.

not placed covers on all emergency shut off switches to protect the simulators from abrupt shutdown.

Management indicated that the decision was made according to the standards at the time of installation. This gives easy access to staff and students alike to power off the simulators in case of an electrical emergency. Management indicated that the TTC will be adding either extender collars or covers to avoid the risk of the emergency shut-off switches being accidentally activated.

- **General Access to the TTC Facility** – The TTC maintained badge access to the facility for individuals not listed as TTC employees. Specifically, we noted an excessive number of individuals[10] had general badge access to all the NRC's facilities (including the NRC's TTC facility), that were not on the TTC employee listing.

  The NRC has not conducted a physical access review of badged access for general access to the TTC facility. NRC management stated that it treats access to the NRC facilities as general access, which it grants to all NRC employees upon onboarding. The NRC Division of Facilities and Security stated that it considers the risk for vetted and badged personnel having general facility access to be extremely low, given the existing mitigations.

  To address this issue, the Division of Facilities and Security stated that, going forward, it will formally document its risk acceptance and reassess this assessment each cycle (i.e., annually) as part of its risk management process.

The NRC Directive Handbook 12.1, *NRC Facility Security Program,* dated April 22, 2024, Section II. Physical Security, directs that access lists (i.e., lists of individuals with authorized access) be required for administratively controlled, limited-access, and security-controlled areas and must be reviewed and approved by the room's designated owner (i.e., the Access Reviewing Official [ARO]) at least annually.

The NRC OCIO Computer Security Standard (CSO-STD-0020), *System Security and Privacy Controls Standard*, dated December 8, 2023, specifies the following related to Physical and Environmental (PE) controls:

- PE-2, *Physical Access Authorization*, requires that the NRC review facility access lists at least annually and that the NRC remove individuals from the facility access lists when those individuals no longer need access.
- PE-4, *Access Control for Transmission*, requires that the NRC control physical access to power distribution; telecommunications transmission lines; and network cabling within organizational facilities using locked wiring closets or locked telephone closets; disconnected or locked spare jacks; conduit or cable trays; and alarms.
- PE-9, *Power Equipment and Cabling*, requires that the NRC protect power equipment and power cabling for the system from damage and destruction.
- PE-10, *Emergency Shutoff*, requires that the NRC protect emergency power shutoff capability from unauthorized activation.

Without properly securing networking equipment and emergency shut-off switches, the NRC increases the risk that important equipment may unintentionally be damaged. In addition,

[10] Details were provided to NRC management for the specific count of individuals identified.

without reviewing badged access to the NRC's TTC facility, the NRC increases the risk that individuals may have unnecessary access to the facility. Further, without removing badged access for individuals who no longer need to access to the facility or who received general badged access without a need to know, the NRC increases the risk of unauthorized access to the facility.

***Recommendation 3**:* We recommend that the NRC's TTC management install a server cage on the second floor of the facility for the NRC Information Technology Infrastructure Patch Panel.

Recommendation 4: We recommend that the NRC's TTC management install protective covers over the emergency power shut-off switches throughout the facility.

Recommendation 5: We recommend that NRC management define and implement a risk-based process for regularly reviewing users who have badged access to the NRC general access group and restricting badged access to the Regions based on business needs.

Recommendation 6: We recommend that NRC management perform a risk-based analysis of the practice of allowing users to have general badge access to multiple NRC facilities. As a part of this risk-based analysis, NRC management should define, document, and implement mitigating controls that reduce the potential impact of having users with badged access to multiple facilities.

APPENDIX A: BACKGROUND

Overview

The NRC's Technical Training Center (TTC) provides training for the NRC staff in various technical disciplines associated with the regulation of nuclear materials and facilities.[11] The TTC office operates under the direction of a Deputy Associate Director within the Office of the Chief Human Capital Officer and is located in Chattanooga, Tennessee.

Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Agencies must also report annually to the Office of Management and Budget and to congressional committees on the effectiveness of their information security program and practices. In addition, FISMA requires agency Inspectors General to assess the effectiveness of their agency's information security program and practices.

National Institute of Standards and Technology Security Standards and Guidelines

FISMA requires the National Institute of Standards and Technology (NIST) to provide standards and guidelines for federal information systems. The prescribed standards include information security standards that provide the minimum information security requirements necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with NIST's Federal Information Processing Standards. In addition, NIST develops and issues Special Publications as recommendations and guidance documents.

[11] https://www.nrc.gov/about-nrc/locations.html

APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this audit was to assess the effectiveness of the information security policies, procedures, and practices of the NRC's TTC.

Scope

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, as issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit included an assessment of the information security programs and practices of the NRC's TTC, consistent with the FISMA for Fiscal Year (FY) 2024. The scope included assessing the following selected security controls from NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*:

Access Controls (AC)
AC-1 Policy and Procedures
AC-2 Account Management
AC-6 Least Privilege
AC-6(5) Privileged Accounts
AC-6(7) Review of User Privileges
AC-6(9) Log Use of Privileged Functions

Audit and Accountability (AU)
AU-1 Policy and Procedures
AU-2 Event Logging
AU-6 Audit Record Review, Analysis, and Reporting

Assessment, Authorization, and Monitoring (CA)
CA-1 Policy and Procedures
CA-2 Control Assessments
CA-5 Plan of Action and Milestones
CA-6 Authorization

Configuration Management (CM)
CM-3 Configuration Change Control
CM-8 System Component Inventory
CM-9 Configuration Management Plan

Contingency Planning (CP)
CP-1 Policy and Procedures
CP-2 Contingency Plan
CP-4 Contingency Plan Testing
CP-9 System Backup

Physical and Environmental Protection (PE)
PE-1 Policy and Procedures
PE-2 Physical Access Authorization (Requirement C – Physical Access Reviews)
PE-6 Monitoring Physical Access
PE-14 Environmental Controls

Planning (PL)
PL-2 System Security and Privacy Plans

Program Management (PM)
PM-5 System Inventory

Risk Assessment (RA)
RA-5 Vulnerability Monitoring and Scanning

We conducted the audit fieldwork remotely from Alexandria, Virginia, and onsite at the TTC facility in Chattanooga, Tennessee, from March 2024 through October 2024.

Methodology

To accomplish our audit objective, we completed the following procedures:

- Evaluated specific controls related to the information security program and practices of the NRC's TTC.
- Inspected security policies, procedures, and documentation.
- Conducted walkthroughs of the TTC facility.
- Performed inquiries of the NRC's TTC and Headquarters management and staff.

In addition, we considered the following NRC OIG audit:

- *Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024* (Report No. OIG-24-A-11, September 30, 2024).[12]

Our work did not include assessing the sufficiency of internal controls over the NRC's TTC's information security program or other matters not specifically outlined in this report.

[12] ROA-OIG-24-A-11-FY-2024-NRC-FISMA.pdf (oversight.gov)

APPENDIX C: MANAGEMENT RESPONSE

NRC management reviewed a discussion draft of this report. On December 13, 2024, NRC management indicated their general agreement with the findings and recommendations of this report and chose not to provide formal comments for inclusion in this report.