MEMORANDUM

DATE: March 31, 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 REGION III: NAPERVILLE, ILLINOIS (OIG-NRC-25-A-06)

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 Region III: Naperville, Illinois*. 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 NRC Region III facility. 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 audit. The agency's staff indicated that they had no formal comments for inclusion in this report.

For the period March 2024 through November 2024, Sikich found that although the NRC generally implemented effective information security policies, procedures, and practices for Region III, the agency's implementation of a subset of selected controls was not fully effective. There are weaknesses in Region III's information security program and practices. As a result, one recommendation was made to assist Region III in strengthening its information security program.

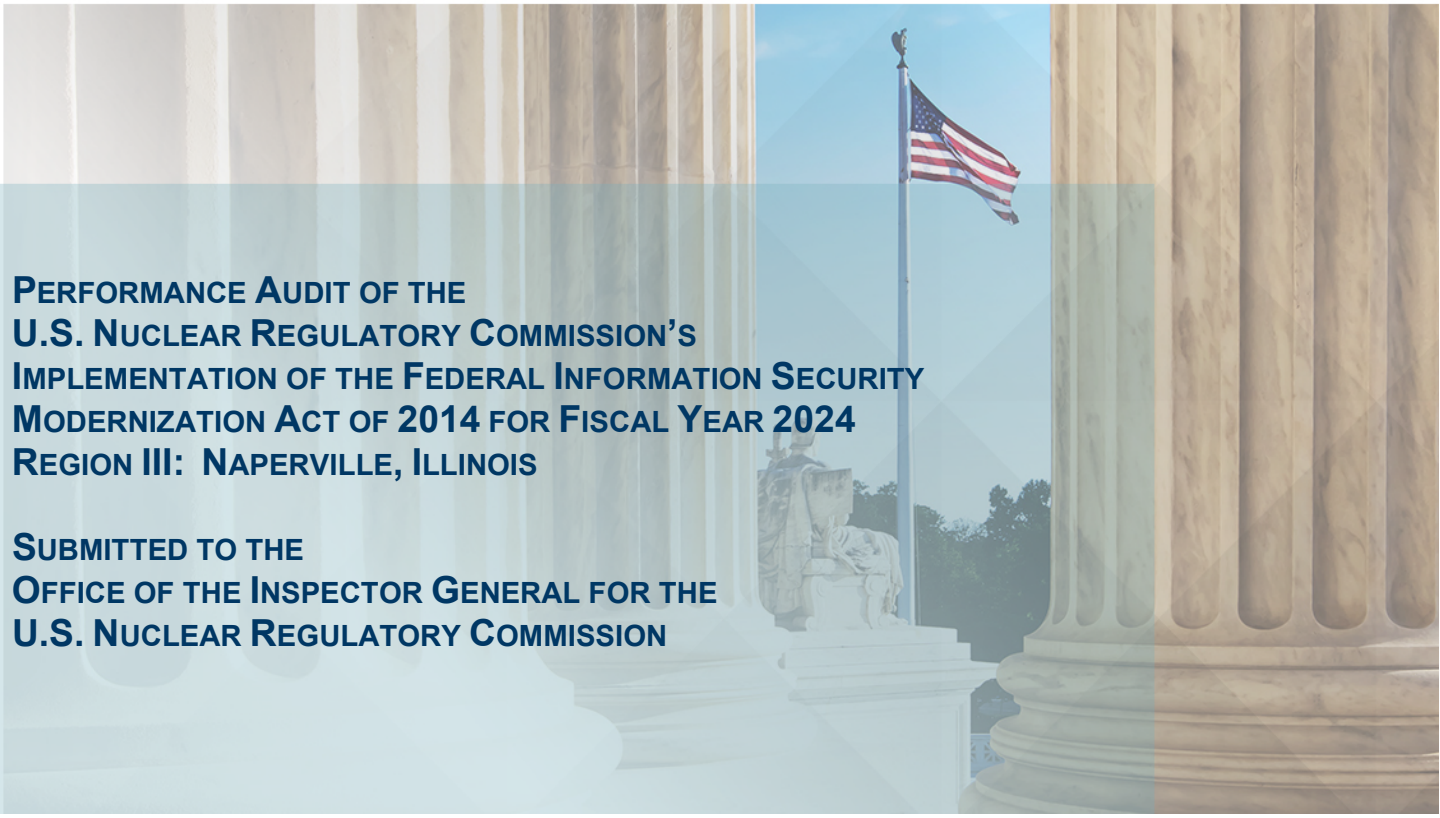
Please provide information on actions taken or planned on the recommendation within 30 calendar days of the date of this report. Actions taken or planned are subject to the OIG follow-up as stated in Management Directive 6.1. We appreciate the cooperation extended to us by members of your staff during 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
D. Lewis, 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 REGION III: NAPERVILLE, ILLINOIS

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

PERFORMANCE AUDIT REPORT

MARCH 31, 2025

ACCOUNTING TECHNOLOGY ADVISORY

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

SIKICH.COM

March 31, 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's) Region III 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's 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 Technical Training Center in its independent evaluation of the NRC's implementation of FISMA for FY 2024. This report presents the audit results for the NRC's Region III. We conducted the audit fieldwork remotely from Alexandria, Virginia, and onsite at the Region III facility in Naperville, Illinois, from March through November 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 the agency's Inspector General to assess the effectiveness of the agency's information security program and practices. The Office of Management and Budget (OMB) 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) has four regional offices that execute agency policies and programs in inspection, enforcement, investigation, licensing, and emergency response programs. To provide an independent evaluation of the NRC's implementation of FISMA for fiscal year (FY) 2024, the NRC's Office of the Inspector General (OIG) engaged Sikich CPA LLC (Sikich) to conduct a performance audit to assess the effectiveness of the information security policies, procedures, and practices for two of the NRC's four regional offices and the NRC's Technical Training Center (TTC). This report presents the audit results for the NRC's Region III.

The audit included an assessment of the NRC's Region III's implementation of select security controls[2] 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 Region III facility in Naperville, Illinois, from March 2024 through November 2024.

II. SUMMARY OF RESULTS

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

- Maintained effective onboarding processes for new hires at Region III.
- Maintained effective physical security controls related to the use of security cameras and security guards.

Although we concluded that the NRC generally implemented effective information security policies, procedures, and practices for Region III, the agency's implementation of a subset of selected controls was not fully effective. We noted weaknesses related to access controls for the employee separation process, physical access controls, and inventory management controls. As a result, we made one recommendation to assist the NRC's Region III in strengthening its information security program.

The following section provides detailed information regarding each finding. **Appendix A** provides background information, and **Appendix B** describes the audit objective, scope, and methodology.

[2] The security controls selected for testing are listed in Appendix B: Objective, Scope, and Methodology.

III. AUDIT RESULTS

Finding 1: The NRC Should Improve Its Separation Processes.

The NRC did not disable the Active Directory accounts of separated Region III employees in a timely manner. Specifically, for the 8 Region III employees separated between October 1, 2023, and August 20, 2024, the NRC disabled the Active Directory accounts between 9 and 262 days after an 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 2 weeks, and the Personnel Security Branch generally takes action within 1 to 2 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.

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 Controls (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.

Due to this audit being part of a series of NRC FISMA reviews, recommendation 1 in 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* (Report No. OIG-NRC-25-A-04, January 24, 2025), addresses this finding. Since a recommendation was noted in the TTC audit, we did not make a duplicate recommendation for this report.

Finding 2: The NRC Should Improve Physical Access Controls at Region III.

We identified the following issue related to physical access controls for the NRC's Region III facility:

- **General Access to the Region III Facility** – Region III maintained badge access to the facility for individuals not listed as Region III employees. Specifically, an excessive number of individuals[3] who were not on the Region III employee listing had general badge access to all the NRC's facilities (including the NRC's Region III facility).

  The NRC has not conducted a physical access review of badged access for general access to the Region III 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's Division of Facilities and Security stated that, given the existing mitigations, it considers the risk of vetted and badged personnel having general facility access to be extremely low.

  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.

NRC Management 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.

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.

Without removing badged access for individuals who no longer need access to the facility, the NRC increases the risk of unauthorized access to the facility.

Due to this audit being part of a series of NRC FISMA reviews, recommendations 5 and 6 in 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* (Report No. OIG-NRC-25-A-04, January 24, 2025), address this finding. Since recommendations were noted in the TTC audit, we did not make duplicate recommendations for this report.

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

Finding 3: Region III Should Improve Its Inventory Management Procedures.

Region III had not maintained a current physical information technology asset inventory[4] to reflect updates to its current inventory, such as location, following the transition to the current Region III facility in September 2024. Specifically, inventories for both the blue and red tags[5] were not current to reflect the new building and specific room location, and included decommissioned assets.

Since the move to the new Region III facility in September 2024, management indicated that an updated inventory of all blue and red tag assets had yet to be conducted due to conflicting priorities with the move.

NRC OCIO Computer Security Standard (CSO- -0020), *System Security and Privacy Controls Standard*, dated December 8, 2023, specifies the following related to Configuration Management (CM) controls:

- CM-8, *System Component Inventory*, requires that the NRC review and update the system component inventory at least annually and update within 30 days of hardware or software changes within the system.

NRC Management Directive 13.1, *Property Management*, states that inventories of all NRC equipment tracked in the Space Property Management System (SPMS) are conducted annually. A Wall-to-Wall (physical inventory) is conducted by both the property custodian and an agency property manager. At Regional offices, the property custodian will conduct the physical inventory using an assigned scanner to scan all blue NRC property tags and upload the scanned results into SPMS.

Without properly identifying the location and accuracy of assets maintained, NRC increases the risk that items may be lost, stolen, or reported that items are no longer in use.

Recommendation 1: We recommend that Region III management conduct a physical asset inventory to reflect the current information technology assets located at Region III.

[4] The inventory consists of equipment, such as laptops, servers, switches, and networking equipment.
[5] The NRC blue and red tags are designated as the unique identifiers for managing IT assets. NRC blue tags are tracked in the Space Property Management System and in Service Now for information technology equipment with an acquisition cost of $2,500 or greater. NRC red tags are tracked in Service Now only for IT assets with an acquisition cost of less than $2,500.

APPENDIX A: BACKGROUND

Overview

The NRC has four regional offices, each operating under the direction of a Regional Administrator. The regional offices execute agency policies and programs in areas such as inspection, enforcement, investigation, licensing, and emergency response programs. These offices are the agency's front line in carrying out its mission and implementing established agency policies and programs nationwide.

The Region III office is located in Naperville, Illinois. Region III's Technology and Information Resources Branch[6] provides information technology/management services, regional computer support, Local Area Network administration, telecommunications services, classified communications, information management/mail processing, document reproductions, vehicle function, property management, and Freedom of Information Act activities.

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 (OMB) and congressional committees on the effectiveness of their information security program and practices. In addition, FISMA requires the 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.

[6] Region III | NRC.gov

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 Region III.

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 Region III, 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 Policies and Procedures
AC-2 Account Management
AC-6 Least Privilege
AC-6(5) Privilege Accounts
AC-6(7) Review of User Privileges
AC-6(9) Log Use of Privilege 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 Actions 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 Region III facility in Naperville, Illinois, from March 2024 through November 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 Region III.
- Inspected security policies, procedures, and documentation.
- Conducted walkthroughs of the Region III facility.
- Performed inquiries of NRC's Region III 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-24-11, September 30, 2024).[7]

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

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

APPENDIX C: MANAGEMENT RESPONSE

NRC management reviewed a discussion draft of this report. On February 24, 2025, 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.