MEMORANDUM

DATE: February 4, 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 IV: ARLINGTON, TEXAS (OIG-NRC-25-A-05)

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 IV: Arlington, Texas*. 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 (NRC) Region IV facility. The findings and conclusions presented in this report are the responsibility of Sikich. The OIG's responsibility is to oversee 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.

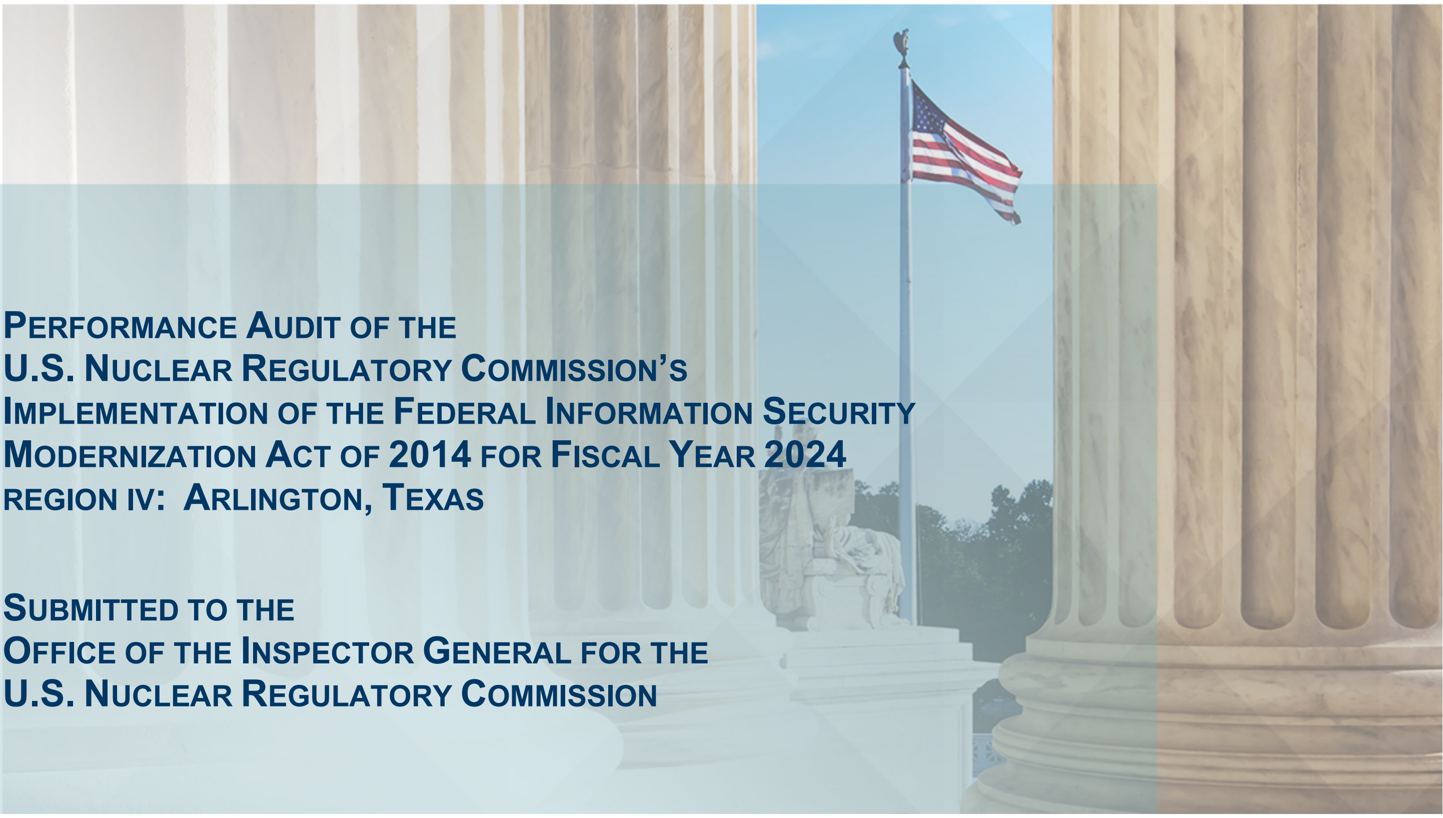
For the period April 2024 through October 2024, Sikich found that although the NRC generally implemented effective information security policies, procedures, and practices for Region IV, the agency's implementation of a subset of selected controls was not fully effective. There were weaknesses in Region IV's information security program and practices. As a result, two recommendations were made to assist Region IV 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
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 IV: Arlington, Texas

Submitted to the
Office of the Inspector General for the
U.S. Nuclear Regulatory Commission

Performance Audit Report

February 4, 2025

SIKICH®

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

SIKICH.COM

February 4, 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 IV 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's 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 IV. We conducted the audit fieldwork remotely from Alexandria, Virginia, and onsite at the Region IV facility in Arlington, Texas, from April 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 (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 areas such as 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 IV.

The audit included an assessment of the NRC's Region IV 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 IV facility in Arlington, Texas, from April through October 2024.

II. Summary of Results

We concluded that the information security policies, procedures, and practices of the NRC's Region IV are generally effective. For example, Region IV:

- Maintained effective physical security controls related to the use of security cameras and security guards, as well as monitoring of visitor access.
- Maintained effective new hire onboarding processes.

Although we concluded that Region IV generally implemented effective information security policies, procedures, and practices, its implementation of a subset of selected controls was not fully effective. We noted weaknesses related to logical and physical access controls and the monitoring of environmental controls. As a result, we made two recommendations to assist either the NRC or Region IV 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.

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

III. AUDIT RESULTS

Finding 1: The NRC Did Not Consistently Disable Inactive User Accounts

Based on our review of the NRC's Active Directory Listing, dated July 15, 2024, we noted that the NRC had not disabled the accounts for 3 network users who had been inactive for more than 90 days. Once we communicated this issue to the NRC, management disabled the accounts.

NRC management stated that the user inactivity script does not take action on accounts that have a null "AltSecID"[3] attribute in Active Directory. This configuration is intentional to ensure that the system does not inadvertently disable service accounts and other accounts that do not record interactive logins. However, if management requests that the NRC retain accounts for departed individuals (for example, to enable management to recover content from the account), these accounts will also have a null "AltSecID" attribute. The Identity, Credential, and Access Management (ICAM) team in the NRC's Office of the Chief Information Officer (OCIO) is investigating methods to enable the NRC to identify inactive accounts using automated processes without inadvertently disabling service accounts.

The NRC's *Information Technology Infrastructure (ITI) Core Services System Security Plan,* dated December 21, 2023, security control Access Controls (AC-2), Enhancement 3, requires that the NRC disable accounts when the accounts have been inactive for more than 90 days. If the NRC does not disable inactive accounts in a timely manner, the NRC may increase the risk of unauthorized access to its information systems and data.

Recommendation 1: We recommend that NRC management investigate methods of identifying inactive user accounts and improving its internal controls over inactivity to ensure that it disables network user accounts after 90 days of inactivity*.*

Finding 2: The NRC Should Improve Its Separation Processes

The NRC's Region IV did not disable the Active Directory accounts of separated employees in a timely manner. Specifically, for 8 of the 10 Region IV employees that separated from October 1, 2023, through June 30, 2024, we noted the following:[4]

- Region IV disabled the Active Directory accounts for 7 separated employees between 38 and 66 days after the employees' effective separation dates.
- Region IV had not disabled the Active Directory account for one of the separated employees at the time of our testing. Based on observation of the NRC's Enterprise Identity Hub (EIH) system, at the time of our testing on July 18, 2024, this user remained active for 145 days past the user's separation date of February 24, 2024.

OCIO management stated that the employee separation process has several dependencies that rely on OCIO, the Office of 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 the accounts

[3] The altSecurityIdentities attribute is a multi-valued attribute that contains mappings for X.509 certificates or external Kerberos user accounts to the user for the purpose of authentication. Refer here for more details.

[4] Eight out of 10 separated Region IV employees had exceptions, while 2 out of 10 separated Region IV employees did not have exceptions.

showed that the EIH automation was correctly disabling accounts on the same day the NRC terminated the employees' 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.

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.
- 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 audits, recommendation 1 in OIG Report: *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 in this report.

Finding 3: The NRC Should Improve Its Physical Access Controls

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

- **Data Center Access Review.** The Region IV – Sensitive Area Access review that the NRC's Region IV performed on October 3, 2023, did not include a review of access to the Region IV data center. Once we notified Region IV management of this issue, Region IV completed an access review of the data center on July 30, 2024.

  Region IV management stated that it had originally begun performing the data center access review at the beginning of FY 2024; however, the responsible party separated from Region IV, and management did not maintain or could not locate evidence of the review.

- **General Access to the Region IV Facility.** Region IV maintained badge access to the facility for individuals not listed as Region IV employees. Specifically, we noted that an excessive number of individuals[5] who were not on the Region IV employee listing had general badge access to all the NRC's facilities (including the Region IV office).

[5] The specific number of individuals identified was provided to NRC management.

The NRC has not conducted a review of badged access for general access to the Region IV facility. NRC management stated that it treats access to the NRC's Region 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.

Management Directive 12.1, *NRC Facility Security Program,* dated April 22, 2024, Section II. Physical Security, requires access lists (i.e., lists of individuals with authorized access) for administratively controlled, limited-access, and security-controlled areas. These lists 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, security control Physical Access Authorization (PE-2), requires that the NRC review facility access lists at least annually and that the NRC remove individuals from the facility access lists when the individuals no longer need access.

Without reviewing badged access to the NRC's Region IV office and its data center, the NRC increases the risk that individuals may have unnecessary access to the Region. In addition, without removing badged access for individuals who no longer need to access the Region or who received general badged access without a need to know, the NRC increases the risk of unintentional access to the facility.

Recommendation 2: We recommend that Region IV management ensure that the Region IV – Sensitive Area Access Review includes the data center and that Region IV management maintains evidence of this review.

Due to this audit being part of a series of NRC FISMA audits, recommendations 5 and 6 in OIG report: *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), partially address this finding. Since recommendations were noted in the TTC audit, we did not make duplicate recommendations in this report.

Finding 4: Region IV Should Improve Its Monitoring of Data Center Environmental Controls

Based on a review of Region IV's Tridium[6] environmental control settings, we noted that Region IV management did not set the data center's high temperature and humidity alarms in accordance with the NRC OCIO Computer Security Standard (CSO-STD-0020), *System Security and Privacy Controls Standard*. Specifically, Region IV management had set the data center's alarms at 80 degrees for temperature and 70 percent for humidity. These levels exceeded the required temperature and humidity ranges of 68 to 75 degrees for temperature

[6] Tridium is software that Region IV uses to monitor environmental controls at its data center, such as controls over humidity and temperature.

and 45 percent to 55 percent for humidity. Once we notified Region IV management of this issue, management corrected the environmental control settings for the data center.

Region IV management stated that this issue occurred as a result of management not being aware of the required alarm settings.

The NRC OCIO Computer Security Standard (CSO-STD-0020), *System Security and Privacy Controls Standard*, dated December 8, 2023, security control Physical and Environmental Protection Control (PE-14), *Environmental Controls*, requires that the NRC monitor temperature and humidity in real-time and maintain a temperature between 68 and 75 degrees and a humidity between 45 percent and 55 percent.

If the NRC does not maintain its information system components (e.g., servers, network equipment) in optimal environmental conditions, it increases the risk that systems may overheat or become damaged, which could ultimately impact the availability of systems and the system components. Because management remediated these weaknesses on-site, we are not issuing recommendations related to this finding.

APPENDIX A: BACKGROUND

Overview

The NRC has four regional offices that each operate 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 IV office is located in Arlington, Texas. Region IV's Technology and Information Resources Branch[7] supports the NRC's and Region IV's mission in the areas of information management, information security, information technology systems support, and telecommunications.

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 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.

[7] Region IV | 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 IV.

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 IV, 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 Region IV facility in Arlington, Texas, from April 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 Region IV.
- Inspected security policies, procedures, and documentation.
- Conducted walkthroughs of the Region IV facility, including its data center.
- Performed inquiries of NRC's Region IV and Headquarters management and staff.

In addition, we took the following NRC OIG audits into consideration:

- *Evaluation of the U.S. Nuclear Regulatory Commission's Information Technology Asset Management* (Report No. OIG-24-E-01, July 3, 2024).[8]
- *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).[9]

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

[8] ROEOIG-24-E-01Evaluation-NRCs-IT-Asset-ManagementHV7324RJF.pdf (oversight.gov)
[9] 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 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.