MEMORANDUM

DATE: January 24, 2024

TO: Daniel H. Dorman
Executive Director for Operations

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

SUBJECT: AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023 REGION I: KING OF PRUSSIA, PENNSYLVANIA (OIG-24-A-03)

The Office of the Inspector General (OIG) contracted with CliftonLarsonAllen LLP (CLA) to conduct the *Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023 Region I: King of Prussia, Pennsylvania*. Attached is CLA'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 I facility. The findings and conclusions presented in this report are the responsibility of CLA. The OIG's responsibility is to provide oversight of the contractor's work in accordance with the 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 October 1, 2022, through September 30, 2023, CLA found that although the NRC Region I generally implemented effective information security policies, procedures, and practices, its implementation of a subset of selected controls was not fully effective. There are weaknesses in Region I's information security program and practices, and as a result, four recommendations were made to assist Region I 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 Avinash Jaigobind, Acting Team Leader, at 301.415.5402.

Attachment:
As stated

cc: M. Bailey, ADO
T. Govan, Acting DADO
J. Jolicoeur, OEDO
OIG Liaison Resource
EDO ACS

Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023

Region I: King of Prussia, Pennsylvania

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
U.S. Nuclear Regulatory Commission

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the U.S. Nuclear Regulatory Commission's (NRC) Region I information security program and practices for fiscal year (FY) 2023 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an agency-wide information security program. In addition, the FISMA requires Inspectors General (IGs) to conduct an annual independent evaluation of their agency's information security program and practices. The NRC Office of the Inspector General (OIG) requested that two of the four NRC regional offices be included in the independent evaluation of the agency's implementation of FISMA for FY 2023. This report describes audit findings for Region I.

The objective of this performance audit was to assess the effectiveness of the information security policies, procedures, and practices of the NRC Region I facility.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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 NRC Region I's information security programs and practices consistent with the FISMA. The scope included assessing selected security controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. Audit fieldwork covered the NRC Region I's facility located in King of Prussia, PA from July 10, 2023, to July 12, 2023. The audit covered the period from October 1, 2022, through September 30, 2023.

We concluded that the NRC Region I information security policies, procedures and practices are generally effective. Although we concluded that Region I generally implemented effective information security policies, procedures, and practices, its implementation of a subset of selected controls was not fully effective. We noted weaknesses in Region I's information security program and practices related to security awareness training, separated user disablement, physical access controls, and vulnerability management. As a result of the weaknesses noted, we made four recommendations to assist Region I in strengthening its information security program.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in this report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. The information included in this report was obtained from the NRC on or before September 30, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring after September 30, 2023.

The purpose of this audit report is to report on our assessment of the NRC Region I's information security policies, procedures, and practices and is not suitable for any other purpose. Additional information on our findings and recommendations are included in the accompanying report.

CliftonLarsonAllen LLP

Arlington, Virginia
November 29, 2023

Table of Contents

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 (IGs) 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 (FIPS) to establish agency baseline security requirements.

The United States (U.S.) Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit to assess the effectiveness of the information security policies, procedures, and practices of the NRC Region I field office.

The NRC has four regional offices that execute agency policies and programs in areas such as inspection, enforcement, investigation, licensing, and emergency response programs. The NRC OIG requested that two of the four NRC regional offices be included in the independent evaluation of the agency's implementation of FISMA for fiscal year (FY) 2023. This report describes audit findings for Region I.

The audit included an assessment of the NRC Region I's implementation of select security controls from the NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. The audit work was conducted during a site visit to Region I in King of Prussia, PA, between July 10, 2023, and July 12, 2023. Any information received from NRC subsequent to the completion of fieldwork was incorporated when possible. The security controls selected for testing are listed in Appendix II – Objective, Scope, and Methodology.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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.

Audit Results

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

- Maintained an effective configuration management program.
- Maintained an effective system assessment and authorization program including an up-to-date system security plan and plan of actions and milestones.
- Maintained an effective contingency planning program including contingency plan testing and system backups.

Although we concluded that Region I generally implemented effective information security policies, procedures, and practices, its implementation of a subset of selected controls was not fully effective. We noted weaknesses in Region I's information security program and practices related to security awareness training, separated user disablement, physical access controls, and vulnerability management. As a result of the weaknesses noted, we made four recommendations to assist Region I in strengthening its information security program.

The following sections provide a detailed discussion of the audit findings. Appendix I provides background information on the FISMA and Appendix II describes the audit objective, scope, and methodology.

AUDIT FINDINGS

1. Weaknesses in Completion of Training Requirements for New Users

For a sample of five new users from the population of 15 new users for Region I, three users did not complete mandatory security awareness training within one week of gaining access to their account.

NRC Region I management indicated delays in the establishment of the Talent Management System account for individuals could cause delays in completion. Additionally, the Region was unaware of the one-week requirement and notifies its new employees to complete training within 30 days.

The Management Directive and Handbook 12.5, *NRC Cybersecurity Program*, states for New NRC Employees and Authenticated Users:

> All new NRC employees shall receive an initial cybersecurity awareness briefing. All NRC authenticated users are required to take the annual cybersecurity awareness course within 1 week of obtaining access to NRC electronic information and annually thereafter.

Without providing adequate security awareness training to individuals, those personnel may not receive proper awareness of risk and procedures for ensuring a secure environment. The NRC may also be at an increased risk of new employees obtaining access to systems without having been made aware of required user actions to help maintain operational security, protect personal privacy, and report suspected incidents.

> ***Recommendation 1:*** *We recommend NRC management implement a process to validate that all new users complete their initial security training requirements and acknowledgement of rules of behavior within the defined timeframes NRC has established.*

2. Weaknesses in Timely Disablement of Separated Individuals

For a sample of five terminated users from the population of nine separated users for Region I, three user accounts were not disabled in a timely manner. The NRC Office of the Chief Information Officer (OCIO) management indicated that the manual processing of exit paperwork and actions caused a delay in the automatic disablement of the accounts.

The NRC Common Control Catalog for NIST SP 800-53 Revision 5, security control implementation details for AC-2 (3): Account Management – Disable Accounts, states:

> The organization disables accounts within [no more than 24 hours] when the accounts:
> 1. Have expired;
> 2. Are no longer associated with a user or individual;
> 3. Are in violation of organizational policy; or
> 4. Have been inactive for [no more than 90-days].

Without consistent disablement of unnecessary user accounts, there is a greater potential risk of individuals gaining unauthorized access to the NRC network environment.

> ***Recommendation 2:*** *We recommend NRC management define and implement a process to notify appropriate members of personnel security of separations at the Region I facility.*

3. Weaknesses in Removal of Unnecessary Badge Access

The Region I office maintained badged access for individuals who were not listed as Region I employees. Specifically, an excessive number of individuals[1] maintained badge access to the Region I facility that were not on the Region I employee listing.

NRC Region I management indicated that the badge access is not removed for individuals who had previously accessed the Region I office. Instead, Region I relies on disablement of the Personal Identifiable Verification (PIV) card at the time of termination or replacement of the PIV is utilized as the control. Additionally, the NRC Security Management and Operations Branch indicated that access to the NRC Region facilities is treated as general access which is granted to all NRC employees upon onboarding.

The NRC Common Control Catalog for NIST SP 800-53 Revision 5, security control implementation details for PE-2: Physical Access Authorizations, states:

> c. Review the access list detailing authorized facility access by individuals [semi-annually] and
> d. Remove individuals from the facility access list when access is no longer required.

Without removal of access for individuals who no longer have a need to access the Region or were granted general access without a need to know, there is an increased risk that unintentional access to the facility could occur.

> ***Recommendation 3:*** *We recommend NRC management define and implement a process to conduct reviews and removal of unnecessary badged access for its Regions.*

4. Weaknesses in Vulnerability Management Process

CLA reviewed the NRC Region I reported vulnerability scan results from June 7th, 2023, and identified Critical and High-risk vulnerabilities related to missing patches, configuration weaknesses, and unsupported software. We provided the list of these vulnerabilities to NRC management and inquired as to their remediation. NRC management provided updated internal vulnerability scan results from September 11, 2023. In comparing the two reports, we identified specific vulnerabilities that were not remediated for over 90 days.

The NRC Common Control Catalog for NIST SP 800-53 Revision 5, security control implementation details for RA-5: Vulnerability Monitoring and Scanning, states:

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

The organization remediates legitimate vulnerabilities in accordance with an organizational assessment of risk;

• Within 30 calendar days for Critical/High vulnerabilities
* * *

NRC OCIO management indicated that they prioritize remediating known exploitable vulnerabilities which results in a relatively low number of repeating vulnerabilities that will be addressed as resources are available. NRC stated that there are legacy requirements for certain software suites that are expected to diminish over time. In addition, certain software versions are required for commercial off the shelf products which NRC is reliant on the vendor to provide updates. Further, NRC has challenges reliably deploying firmware to endpoints.

By timely remediation of identified vulnerabilities, NRC can mitigate security weaknesses and limit the potential for attackers to compromise the confidentiality, integrity, and availability of sensitive data. This ultimately will improve the overall security posture of NRC information systems.

> ***Recommendation 4:*** *We recommend NRC management remediate identified vulnerabilities in accordance with NRC's defined timeframes and document risk acceptances with mitigating controls for vulnerabilities that cannot be remediated within the defined timeframes.*

BACKGROUND

Overview

The Energy Reorganization Act of 1974 created the NRC, and the NRC began operations on January 19, 1975. The NRC's mission is to "license and regulate the Nation's civilian use of radioactive materials to protect public health and safety, promote the common defense and security, and protect the environment."

The NRC has four regional offices that execute agency policies and programs in areas such as inspection, enforcement, investigation, licensing, and emergency response programs. The regional offices are the agency's front line in carrying out its mission and implementing established agency policies and programs nationwide. The Region I office operates under the direction of a Regional Administrator and is located in King of Prussia, Pennsylvania. The region covers an 11-state area and the District of Columbia, including 8 states with nuclear power plants. Region I also oversees materials licensees in Region II.

Federal Information Security Modernization Act of 2014 (FISMA)

The FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting federal operations and assets. The 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.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. The FISMA requires agency heads to take the following actions, among others:[2]

1. Be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems; complying with applicable governmental requirements and standards; and ensuring information security management processes are integrated with the agency's strategic, operational, and budget planning processes.
2. Ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control.
3. Delegate to the agency Chief Information Officer the authority to ensure compliance with FISMA.
4. Ensure that the agency has trained personnel sufficient to assist the agency in complying with FISMA requirements and related policies, procedures, standards, and guidelines.
5. Ensure that the Chief Information Officer reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

[2] 44 U.S.C. § 3554, Federal agency responsibilities.

6. Ensure that senior agency officials carry out information security responsibilities.
7. Ensure that all personnel are held accountable for complying with the agency-wide information security program.

Agencies must also report annually to the OMB and to congressional committees on the effectiveness of their information security program. In addition, the FISMA requires agency IGs to assess the effectiveness of their agency's information security program and practices.

NIST Security Standards and Guidelines

The FISMA requires NIST to provide standards and guidelines pertaining to Federal information systems. The prescribed standards establish minimum information security requirements necessary to improve the security of Federal information and information systems. The FISMA also requires that Federal agencies comply with Federal Information Processing Standards issued by NIST. In addition, NIST develops and issues Special Publications as recommendations and guidance documents.

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 Region I facility.

Scope

We conducted this performance audit in accordance with generally accepted government auditing standards. 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 NRC Region I's information security programs and practices consistent with the FISMA for FY 2023. The scope included assessing the following selected security controls from NIST SP 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-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

The audit work was conducted during a site visit at Region I located in King of Prussia, PA, between July 10, 2023, and July 12, 2023. Any information received from NRC subsequent to the completion of fieldwork was incorporated when possible. The audit covered the period from October 1, 2022, through September 30, 2023.

Methodology

To determine if the NRC Region I implemented an effective information security program, we conducted interviews with NRC Region I and Headquarters officials and reviewed legal and regulatory requirements stipulated in the FISMA. Also, we reviewed documents supporting the information security program. These documents included, but were not limited to, the NRC Region I's (1) information security plan; (2) contingency planning policies and procedures; (3) access control procedures; (4) configuration management procedures; and (5) system generated account listings. Where appropriate, we compared documents, such as the NRC Region I's information technology (IT) policies and procedures, to requirements stipulated in NIST SPs. We also performed tests of system processes to determine the adequacy and effectiveness of those controls.

In addition, our work in support of the audit was guided by applicable NRC policies and Federal criteria, including, but not limited to, the following:

- *Government Auditing Standards* (April 2021).
- CISA's BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities.*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* for specification of security controls (December 10, 2020).
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations,* for the assessment of security control effectiveness.
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy,* for the risk management framework controls (December 2018).
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) (February 2014).
- NRC's policies and procedures, including but not limited to:
  - *NRC Common Controls (NRCcc)-Information Security Program Plan (ISPP).*
  - *Region Information System – Region I System Security Plan.*
  - *Region Information System - Region I Contingency Plan.*
  - Management Directive and Handbook 12.5, *NRC Cybersecurity Program.*

U.S. Nuclear Regulatory Commission
FY 2023 Region I Site FISMA Audit

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk and the significance or criticality of the specific items in achieving the related control objective. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population.

NRC's MANAGEMENT COMMENTS

An exit briefing was held with the Region I management on July 12, 2023. In addition, NRC management reviewed a discussion draft and provided editorial comments that have been incorporated into this report as appropriate. As a result, NRC management stated their general agreement with the findings and recommendations of this report and chose not to provide formal comments for inclusion in this report.