MEMORANDUM

DATE: September 30, 2024

TO: Mirela Gavrilas
Executive Director for Operations

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

SUBJECT: AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2024 (OIG-24-A-11)

The Office of the Inspector General (OIG) contracted with Sikich 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 2024*. 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). 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. Following the exit conference, the agency's staff stated that they had no formal comments for inclusion in this report.

Based on its assessment of the period October 1, 2023, through June 30, 2024, Sikich found that although the NRC has established an effective agency-wide information security program and effective information security practices, there are weaknesses that may have some impact on the agency's ability to optimally protect the NRC's systems and information.

Within 30 calendar days of the date of this report, please provide information on actions taken or planned on each of the report's recommendations. Actions taken or planned are subject to OIG follow-up as stated in Management Directive 6.1.

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.

We appreciate the cooperation extended to us by members of your staff during the audit.

Attachment:
As stated

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

PERFORMANCE AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2024

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

PERFORMANCE AUDIT REPORT

SEPTEMBER 30, 2024

ACCOUNTING TECHNOLOGY ADVISORY

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

SIKICH.COM

September 30, 2024

The Honorable Robert J. Feitel
Inspector General
U.S. Nuclear Regulatory Commission and
Defense Nuclear Facilities Safety Board

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) information security program and practices for fiscal year 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 program 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 engaged Sikich to conduct this performance audit.

The audit covered the period from October 1, 2023, through June 30, 2024. We performed the work from January through June 2024.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, 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 provided by NRC management and staff.

Sincerely,

Sikich CPA LLC

September 30, 2024

[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 U.S. Nuclear Regulatory Commission.

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 (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 to establish agency baseline security requirements.

The Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) engaged Sikich CPA LLC (Sikich)[2] to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of the NRC's information security program and practices. The objective of this performance audit was to assess the effectiveness of the NRC's information security policies, procedures, and practices.

The OMB and the Department of Homeland Security (DHS) annually provide federal agencies and IGs with instructions for preparing FISMA reports. On December 4, 2023, the OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*.[3] This memorandum describes the methodology for conducting FISMA audits and the process for federal agencies to report to the OMB and, where applicable, the DHS. According to that memorandum, each year the IGs are required to complete the IG FISMA Reporting Metrics[4] to independently assess their agency's information security program.

For this year's review, IGs were required to assess 20 core[5] and 17 supplemental[6] IG FISMA Reporting Metrics across five security function areas—Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agency's information security program and the maturity level of each function area. The maturity levels are Level 1: *Ad Hoc*, Level 2: *Defined*, Level 3: *Consistently Implemented*, Level 4: *Managed and Measurable*, and Level 5: *Optimized*. To be considered effective, an agency's information security program must be rated Level 4: *Managed and Measurable*. See **Appendix A** for background information on the FISMA reporting requirements.

For this audit, we reviewed selected controls outlined in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the FY 2024 IG FISMA reporting metrics, for a sample of 3 out of 15 information systems[7] in the NRC's FISMA reportable system inventory as of January 4, 2024. Audit

[2] 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 U.S. Nuclear Regulatory Commission.
[3] See OMB M-24-04 online here.
[4] See the Fiscal Year (FY) 2023 – 2024 IG FISMA Reporting Metrics online here. We submitted our responses to the FY 2024 IG FISMA Reporting Metrics to the NRC OIG as a separate deliverable under the contract for this audit.
[5] Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.
[6] Supplemental metrics are assessed at least once every two years; they represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.
[7] According to the NIST Glossary, an information system is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

fieldwork was performed from January through June 2024. The audit covered the period from October 1, 2023, through June 30, 2024.

II. SUMMARY OF RESULTS

We concluded the NRC implemented effective information security policies, procedures, and practices, since the NRC achieved an overall maturity level of Level 4: *Managed and Measurable*. Therefore, the NRC's information security program is considered effective. **Table 1** below summarizes the overall maturity levels for each security function and domain in the Fiscal Year (FY) 2024 IG FISMA Reporting Metrics.

Table 1: Maturity Levels for FY 2024 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Maturity Level by Function	Domain	Maturity Level by Domain
Identify	Level 4: *Managed and Measurable*	Risk Management	Level 5: *Optimized* (Effective)
		Supply Chain Risk Management	Level 2: *Defined* (Not Effective)
Protect	Level 3: *Consistently Implemented*	Configuration Management	Level 3: *Consistently Implemented* (Not Effective)
		Identity and Access Management	Level 3: *Consistently Implemented* (Not Effective)
		Data Protection and Privacy	Level 4: *Managed and Measurable* (Effective)
		Security Training	Level 3: *Consistently Implemented* (Not Effective)
Detect	Level 4: *Managed and Measurable*	Information Security Continuous Monitoring	Level 4: *Managed and Measurable* (Effective)
Respond	Level 4: *Managed and Measurable*	Incident Response	Level 4: *Managed and Measurable* (Effective)
Recover	Level 4: *Managed and Measurable*	Contingency Planning	Level 4: *Managed and Measurable* (Effective)
Overall	**Level 4: *Managed and Measurable* (Effective)**		

Source: Sikich's assessment of the NRC's information security program controls and practices based on the FY 2024 IG FISMA Reporting Metrics.

We found that the NRC established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, the NRC:

- Maintained an effective risk management program with a centralized information system inventory that leverages a combination of cybersecurity risk framework profiles, risk assessments, and advanced technologies for trend analysis and benchmarking to support risk-based decision-making.
- Maintained an effective continuous monitoring program including periodic security control assessments, dashboards for tracking risk posture and metrics for situational awareness.
- Maintained an effective incident response program that leverages qualitative and quantitative performance measures for data driven decision making on incident handling.

Notwithstanding these actions, our report describes control weaknesses that reduced the effectiveness of the NRC's information security program and practices, as follows:

- The NRC needs to complete the enrollment of personnel in continuous vetting to replace the performance of periodic reinvestigations (Finding 1: Protect Function – Identity and Access Management Domain).
- The NRC needs to improve how security and privacy training program assignments are managed and enforced (Finding 2: Protect Function – Security Training Domain).

In addition, the NRC has outstanding prior-year recommendations that impact the IG FISMA Reporting Metrics. Specifically, at the beginning of FY 2024, the NRC had 40 open recommendations from prior FISMA audits and evaluations dating from 2019 through 2023. During our FY 2024 audit, we found that the NRC took corrective actions to address 19 recommendations, and we consider those recommendations closed. Corrective actions are in progress for the other 21 open recommendations.

As a result of the weaknesses noted, we made four new recommendations to assist the NRC in strengthening its information security program. Additionally, we noted that 21 prior-year recommendations remain open.[8]

The following section provides a detailed discussion of the audit results. **Appendix A** provides background information on FISMA. **Appendix B** describes the audit objective, scope, and methodology. **Appendix C** provides the status of prior-year recommendations. **Appendix D** includes management's response.

III. AUDIT RESULTS

The following section of the report describes the key controls underlying each function and domain and our assessment of the NRC's implementation of those controls. We have organized our conclusions and ratings by function area and domain to help orient the reader to deficiencies as categorized by NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).

Security Function: Identify

The objective of the Identify function is to develop an organizational understanding of the business context and the resources that support critical functions for managing cybersecurity risk to systems, people, assets, data, and capabilities. We determined that the maturity level of the NRC's Identify function is Level 4: *Managed and Measurable*.

Risk Management

An agency with an effective risk management program maintains an accurate inventory of information systems, hardware assets, and software assets; consistently implements its risk management policies, procedures, plans, and strategy at all levels of the organization; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk management program.

We determined that the maturity level of the NRC's Risk Management domain is Level 5: *Optimized*. The NRC has used automation to develop and maintain a near real-time centralized information system inventory, adopted cybersecurity framework profiles to support risk-based

[8] See Appendix C for the status of prior-year recommendations.

decision making, and institutionalized the use of advanced technologies for trend analysis and benchmarking for continuous improvement of its risk management program.

However, we noted that the NRC has four open prior-year recommendations in the Risk Management domain related to the (1) management of plans of action and milestones (POA&M), (2) ensuring external interconnections in the Information Technology Infrastructure (ITI) Core System Security Plan have documented interconnection security agreements, (3) improving the ITI subsystem inventory management, and (4) using a formally developed information security architecture to make updates to their risk tolerance and appetite levels at the enterprise, business process, and information system levels as necessary.[9]

Supply Chain Risk Management

An agency with an effective supply chain risk management program ensures that external providers' products, system components, systems, and services are consistent with the agency's cybersecurity and supply chain risk management requirements. It also reports qualitative and quantitative performance measures on the effectiveness of its supply chain risk management program.

We determined that the maturity level of the NRC's Supply Chain Risk Management domain is Level 2: *Defined*. The NRC implemented a supply chain risk management strategy. However, we noted that the NRC has five open prior-year recommendations in the Supply Chain Risk Management domain, with emphasis on finalizing the implementation of supply chain risk assessment processes, counterfeit component detection and prevention, and supply chain integration with contingency planning processes.[10]

Security Function: Protect

The objective of the Protect function is to develop and implement safeguards to ensure the delivery of critical infrastructure services, and to prevent, limit, or contain the impact of a cybersecurity event. We determined that the maturity level of the NRC's Protect function is Level 3: *Consistently Implemented*.

Configuration Management

An agency with an effective configuration management program employs automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; consistently implements its configuration management policies, procedures, plans, and strategy at all levels of the organization; centrally manages its flaw remediation process; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its configuration management program.

We determined that the maturity level of the NRC's Configuration Management domain is Level 3: *Consistently Implemented* based on the results of the core metrics. The NRC demonstrated strengths in the supplemental metrics for this domain by using automation to adapt its configuration management plan and its related processes, activities, roles, and responsibilities to a changing cybersecurity landscape. The NRC also used automation to improve the

[9] See Appendix C for additional information regarding these prior-year recommendations.
[10] See Appendix C for additional information regarding these prior-year recommendations.

accuracy, consistency, and availability of configuration change control and configuration baseline information.

However, we noted that the NRC has two open prior-year recommendations in the Configuration Management domain[11] that relate to improving its patch and vulnerability management program. In addition, our POA&M analysis for one out of three sampled systems found that the NRC has open POA&Ms related to configuration settings, least functionality, and flaw remediation requirements.

Identity and Access Management

An agency with an effective identity and access management program ensures that all privileged and non-privileged users employ strong authentication for accessing organizational systems; uses automated mechanisms to support the management of privileged accounts; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its identity, credential, and access management program.

We determined that the maturity level of the NRC's Identity and Access Management domain is Level 3: *Consistently Implemented.* The NRC demonstrated strengths in this area by implementing multi-factor authentication for network access for both non-privileged and privileged users and by consistently managing privileged user access rights and activity.

However, we found that the NRC has opportunities to improve its Identity and Access Management program by implementing the three open prior-year recommendations in this domain.[12] These recommendations emphasize the implementation requirements across all event logging maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021). These recommendations also relate to completing updates to all applicable policies and procedures to incorporate requirements for signing rules of behavior and non-disclosure agreements before granting access to systems.

Additionally, we noted the following regarding NRC personnel enrollment in continuous vetting.

Finding 1: The NRC Needs to Complete Its Enrollment of Personnel in Continuous Vetting.

At the time of our review, the NRC had not yet completed the enrollment of all individuals occupying national security positions in continuous vetting in accordance with Office of Personnel Management (OPM) requirements. Based on our inspection of the current enrollment status of NRC personnel in continuous vetting, we noted there were 214 individuals, consisting of 193 NRC employees and 21 NRC contractors, with either a "Q" or "L" clearance

[11] See Appendix C for additional information regarding these prior-year recommendations.
[12] See Appendix C for additional information regarding these prior-year recommendations.

level[13] required for their positions, that were neither enrolled in Trusted Workforce (TW)[14] nor Department of Defense Continuous Vetting (DoD CV)[15] by September 30, 2022, in accordance with OPM guidance.

The OPM Memorandum, *Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0* (January 15, 2021), requires that individuals occupying national security positions (i.e., Tier 3 and Tier 5) be enrolled in Trusted Workforce by September 30, 2022.

The Directive Handbook to NRC Management Directive (MD) 12.3, *NRC Personnel Security Program* (July 18, 2022), Section I, "NRC Access Types," Subsection B, "Position Sensitivity Criteria," also states, "Position sensitivity criteria determine whether a person in a particular NRC position requires a 'Q' or a high public trust 'L(H)' security clearance based on a Tier 5 (T5) investigation by the agency's investigation service provider, or the equivalent conducted by other Federal agencies, or an 'L' security clearance, as a minimum, based on a Tier 3 (T3) investigation or equivalent."

Officials from the NRC's Office of Administration, Division of Facilities and Security, Personnel Security Branch noted that the continuous vetting enrollment process is inherently manual in terms of data entry and communication of requests to the Defense Counterintelligence and Security Agency (DCSA). NRC management also noted that the inherently manual nature of the continuous vetting enrollment process may introduce a potential for human error in the process. Furthermore, the implementation and enrollment of the NRC's employees and contractors (as appropriate) in TW remains a work in progress. It is intended that TW will ultimately replace the need for existing legacy reinvestigations, once the NRC adoption of continuous vetting is complete.

Without effective tracking of background reinvestigation data for employees and contractors through continuous vetting, there is a risk that they may not be reinvestigated under the manual reinvestigation process. Therefore, the NRC is potentially at risk of allowing unnecessary or unauthorized access to sensitive systems and data for individuals that were not enrolled in TW or DoD CV.

Therefore, we recommend that the NRC's Office of Administration, Division of Facilities and Security, Personnel Security Branch, in coordination with the Office of the Chief Human Capital Officer:[16]

[13] Directive Handbook 12.3, *NRC Personnel Security Program*, Exhibit 4, states that: the Q – Top Secret security clearance requires a Tier 5 investigation (T5), with Tier 5 Reinvestigation (T5R) every 5 years (if applicable); the L – High Public Trust (L(H)) (Secret) security clearance requires a T5 with Tier 3 Reinvestigation (T3R) every 5 years (if applicable); and the L – Secret (S) security clearance requires a Tier 3 investigation (T3) with T3R every 10 years (if applicable).

[14] Enrollment in TW means that an individual will undergo continuous vetting instead of periodic reinvestigations. Continuous vetting involves regular reviews of a cleared individual's background to confirm they will still meet eligibility requirements to maintain their security clearance. Continuous vetting also helps address personnel security issues proactively, potentially mitigating risks or, in some instances, suspending or revoking clearances if necessary (summarized information from OPM Trusted Workforce 2.0 Transition Memorandum Appendix 1).

[15] Enrollment in DoD CV in lieu of TW means that an NRC employee or contractor is either a reservist or a transfer from the DoD to NRC.

[16] In comments provided by agency management on September 12, 2024, the NRC stated that "DCSA is building an automated system that will enroll individuals into CV when the clearance is granted by the NRC, eliminating the manual process and negating the possibility of individuals failing to be enrolled. The list of 214 individuals were submitted for enrollment as of June 21, 2024. Any individuals who cannot be enrolled due to age of their previous

Recommendation 1: Implement a process to monitor and ensure that reinvestigations occur for the identified employees and contractors not currently enrolled in continuous vetting through either TW or DoD CV until such time as their enrollment is complete.

Recommendation 2: Complete enrollment of the identified employees and contractors in continuous vetting through TW.

Data Protection and Privacy

An agency with an effective data protection and privacy program maintains its data's confidentiality, integrity, and availability; can assess its security and privacy controls, as well as its breach response capacities; and reports on qualitative and quantitative data protection and privacy performance measures.

We determined that the maturity level of the NRC's Data Protection and Privacy domain is Level 4: *Managed and Measurable.* The NRC demonstrated strengths in this area by protecting data throughout its lifecycle (i.e., at rest, in transit, and through destruction) and by fully integrating data exfiltration, enhanced network defenses and the data breach response plan into risk management, information security continuous monitoring, and incident response programs.

However, we noted that the NRC has two open prior-year recommendations in this area related to developing and implementing role-based privacy training.[17] Additionally, the NRC's privacy training program needs improvement, as noted below in Finding 2 in the *Security Training* section.

Security Training

An agency with an effective security training program identifies and addresses gaps in security knowledge, skills, and abilities; measures the effectiveness of its security awareness and training program; and ensures staff consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

We determined that the maturity level for the NRC's Security Training domain is Level 3: *Consistently Implemented*. The NRC has shown strengths in this area by conducting a workforce assessment, collecting feedback on general security and role-based training content, conducting targeted phishing exercises, and monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its security training.

However, we noted that the NRC has five open prior-year recommendations in this area related to the assignment and completion of security awareness and role-based training, as applicable.[18]

Additionally, we noted the following related to the assignment or timely completion of initial Cybersecurity Awareness (CSA) and Personally Identifiable Information and Privacy Act (PII) training in Talent Management System (TMS) for NRC employees and contractors.

---

investigation or age of their security documents will be reinvestigated." The OIG will follow up on implementation of corrective actions through the status of recommendations process in coordination with the FY 2025 FISMA audit.

[17] See Appendix C for additional information regarding these prior-year recommendations.

[18] See Appendix C for additional information regarding these prior-year recommendations.

Finding 2: The NRC Needs to Improve How Security and Privacy Training Program Assignments Are Managed and Enforced.

We reviewed initial CSA and PII training records for a sample of 20 new hires since October 1, 2023, consisting of 6 employees and 14 contractors. Based on our review, we noted the following discrepancies regarding the assignment or timely completion of their initial CSA and PII training:

- Six out of 20 sampled new hires (5 employees and 1 contractor) did not complete their CSA training within one week of obtaining access to NRC electronic information as required by NRC policy.
- Five contractors out of 20 sampled new hires were inactive in TMS and did not have their mandatory initial CSA and PII training assigned or completed.

The Directive Handbook to NRC MD 12.5, *NRC Cybersecurity Program* (October 2020), Section IV, "Personnel," Subsection C, "Cybersecurity Awareness, Training, and Education," states, in part:

> *2. New NRC Employees and Authenticated Users*
> *…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.*

NRC *Privacy Program Plan* (September 2020) Section 10, "Awareness and Training," also states, in part, "NRC requires all employees and contractors to complete privacy training when first beginning work with the Agency and annually thereafter."

At the time of our review, NRC management stated that the current requirement to complete CSA training within one week of obtaining access to NRC electronic information is being reviewed and reconsidered. NRC management also stated that a workaround to the current requirement was underway but had not yet been implemented agency wide.

With regard to the assignment of initial CSA and PII training, under the current configuration of the TMS integration with the Enterprise Identity Hub (EIH), TMS account status is tied to Active Directory (network) account status, meaning that TMS accounts are set to inactive when Active Directory (network) accounts are disabled due to inactivity. When TMS accounts are set to inactive, training assignments are cancelled.

Without providing adequate security awareness and privacy training to individuals, those personnel may be unaware of risks and the procedures for ensuring a secure environment. The NRC may also be at an increased risk of new contractors or new employees obtaining access to systems without reading, understanding, and agreeing to abide by rules of behavior and without having been made aware of required user actions to help maintain operational security, protect personal privacy, and report suspected incidents.

We recommend the Office of the Chief Human Capital Officer and Office of the Chief Information Officer:

Recommendation 3: Review and update the organizationally defined timeframe for completion of security training in NRC MD 12.5.[19]

Recommendation 4: Implement a technical capability to capture NRC employees' and contractors' initial login dates so that the required cybersecurity awareness and role-based training can be accurately tracked and managed by the current process. Also, as part of this recommendation, consider reviewing the current configuration of the EIH and TMS integration—as well as the logic in TMS itself, as necessary—to ensure training assignments are retained (not cancelled) due to inactivity.

Security Function: Detect

The objective of the Detect function is to implement continuous monitoring of control activities to discover and identify cybersecurity events in a timely manner. Cybersecurity events[20] include anomalies and changes in the organization's IT environment that may impact organizational operations, including operations tied to the organization's mission, capabilities, or reputation. We determined that the maturity level of the NRC's Detect function is Level 4: *Managed and Measurable.*

Information Security Continuous Monitoring

An agency with an effective information security continuous monitoring program maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its information security continuous monitoring program into agency programs in a manner that delivers persistent situational awareness across the organization; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its information security continuous monitoring policies, procedures, plans, and strategies.

We determined that the maturity level for the NRC's Information Security Continuous Monitoring domain is Level 4: *Managed and Measurable.* The NRC has shown strengths in this area by leveraging the results of periodic security control assessments and continuous monitoring activities to maintain ongoing authorizations of information systems. The NRC has also shown strength in this area by monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its information security continuous monitoring policies and strategy and making updates, as appropriate. Furthermore, the NRC has illustrated the capability to actively adapt its information security continuous monitoring program to a changing cybersecurity landscape on a near real-time basis.

However, the integration of the supply chain risk management strategy with the information security continuous monitoring program represents a key opportunity for improvement in this

[19] In comments provided by agency management on September 12, 2024, NRC stated, "The NRC has implemented a process to validate that all new contractor personnel complete their initial security training requirements and acknowledgement of the rules of behavior within 20 business days of obtaining access to the NRC systems, and annually thereafter. The change in timeline was updated in our Management Directive Reference: MD 12.5. Additionally, we will ensure the tracking of the completion of annual security awareness training and renewal of the rules of behavior. This activity is monitored in the TMS." Although the NRC considers this finding remediated, we noted that the new version of NRC MD 12.5 was issued July 29, 2024, and any related new or revised control(s) were therefore implemented outside the audit period from October 1, 2023, through June 30, 2024. Thus, the OIG will follow-up on implementation of corrective actions through the status of recommendations process in coordination with the FY 2025 FISMA audit.

[20] https://csrc.nist.gov/glossary/term/cybersecurity_event

domain, as noted in the *Supply Chain Risk Management* section above. There were no prior-year recommendations that directly map back to this domain.

Security Function: Respond

The objective of the Respond function is to implement processes to contain the impact of detected cybersecurity events. Such processes include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. We determined that the maturity level of the NRC's Respond function is Level 4: *Managed and Measurable*.

Incident Response

An agency with an effective incident response program:

- Utilizes profiling techniques to measure the characteristics of expected network and system activities so it can more effectively detect security incidents.
- Manages and measures the impact of successful incidents.
- Utilizes incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.
- Consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies.

We determined that the maturity level of the NRC's Incident Response domain is Level 4: *Managed and Measurable.* The NRC monitors and analyzes the qualitative and quantitative performance measures to monitor and maintain the effectiveness of its overall incident response capability. The NRC also continuously evaluates and adapts its incident response-based roles and responsibilities to account for a changing cybersecurity landscape.

However, the NRC has an open recommendation in this area related to implementing requirements across all event logging maturity tiers to ensure that it logs and tracks events in accordance with OMB M-21-31.[21]

Security Function: Recover

The objective of the Recover function is to develop and implement activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity incident. The Recover function supports the timely recovery of normal operations to reduce the impact of a cybersecurity incident; this function includes recovery planning, improvements, and communications.

We determined that the maturity level of the NRC's Recover function is Level 4: *Managed and Measurable*.

Contingency Planning

An agency with an effective contingency planning program establishes contingency plans; employs automated mechanisms to thoroughly and effectively test system contingency plans;

[21] See Appendix C for additional information regarding these prior-year recommendations.

communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures regarding the effectiveness of information system contingency planning program activities.
We determined that the maturity level for the NRC's Contingency Planning domain is Level 4: *Managed and Measurable.* The NRC has documented organization and system level Business Impact Analyses (BIAs) and contingency plans. The NRC has also performed contingency plan testing and exercises, including testing that integrates with related plans such as their incident response plan to the extent practicable. In addition, the NRC has shown that information system backups are performed, backup storage is safeguarded, and alternate storage and processing sites are used when necessary.
However, we noted that the NRC has three open prior-year recommendations in the Contingency Planning domain[22] related to the following:

- Expanding the integration and use of contingency planning metrics to include mean time to recovery, incident response time, and site recovery time.
- Developing and implementing testing of contingency plans using automated mechanisms, if feasible and cost effective.
- Updating contingency planning policies and procedures to address Information and Communications Technology (ICT) supply chain risk.

[22] See Appendix C for additional information regarding these prior-year recommendations.

APPENDIX A: BACKGROUND

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 OMB and Congressional committees on the effectiveness of their information security program and practices. In addition, FISMA requires agency IGs to assess the effectiveness of their agency's information security program and practices.

NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to federal information systems. The standards prescribed include information security standards that provide minimum information security requirements necessary to improve the security of federal information and information systems. 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.

FISMA Reporting Requirements

The OMB and the DHS annually provide federal agencies and IGs with instructions for preparing FISMA reports. On December 4, 2023, the OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the methodology for conducting FISMA audits and the processes for federal agencies to report to the OMB and, where applicable, the DHS. The methodology includes the following:

- The OMB selected 17 supplemental IG FISMA Reporting Metrics that IGs must evaluate during FY 2024, in addition to the 20 core IG FISMA Reporting Metrics that IGs must evaluate annually. The remainder of the standards and controls are evaluated on a 2-year cycle.
- In previous years, IGs have been directed to utilize a mode-based scoring approach to assess maturity levels. Beginning in FY 2023, ratings were focused on calculated average scores, wherein IGs would use the average of the metrics in a particular domain to determine the effectiveness of the individual function areas (i.e., Identify, Protect, Detect, Respond, and Recover). The OMB encouraged IGs to focus on the calculated average scores of the 20 core IG FISMA Reporting Metrics, as these tie directly to the administration's priorities and other high-risk areas. In addition, the FY 2024 IG FISMA Reporting Metrics stated that IGs should use the calculated average scores of the supplemental IG FISMA Reporting Metrics and the agency's progress in addressing outstanding prior-year recommendations as data points to support their risk-based determination of the overall effectiveness of the program and function level.

For this year's review, IGs were to assess the 20 core and 17 supplemental IG FISMA Reporting Metrics in the 5 security function areas to determine the maturity level and effectiveness of their agency's information security program. As highlighted in **Table 2**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST Cybersecurity Framework, version 1.1: Identify, Protect, Detect, Respond, and Recover.

Table 2: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2024 IG FISMA Reporting Metrics

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Identify	Develop an organizational understanding of the business context and the resources that support critical functions to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Risk Management and Supply Chain Risk Management**
Protect	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**
Detect	Implement activities to identify the occurrence of cybersecurity events.	**Information Security Continuous Monitoring**
Respond	Implement processes to take action regarding a detected cybersecurity event.	**Incident Response**
Recover	Implement plans for resilience to restore capabilities or services impaired by a cybersecurity event.	**Contingency Planning**

Source: Sikich's analysis of the NIST Cybersecurity Framework and IG FISMA Reporting Metrics.

The foundational levels of the maturity model in the IG FISMA Reporting Metrics focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 3** explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of Level 4: *Managed and Measurable*.

Table 3: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2024 IG FISMA Reporting Metrics

APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

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

Scope

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, 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.

The scope of this performance audit covered the NRC's information security program and practices consistent with FISMA and reporting instructions that the OMB and the DHS issued for FY 2024. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, to support the FY 2024 IG FISMA Reporting Metrics, for a sample of 3 out of 15 information systems in the NRC's FISMA reportable system inventory as of January 4, 2023, as highlighted in **Table 4**.

Table 4: Description of Systems Selected for Testing

System Name	Description
Information Technology Infrastructure (ITI) System	ITI is a General Support System (GSS) that supports the NRC's mission by providing the networking backbone, connectivity, office automation, remote access services, and information security functions to include intrusion detection, malicious code protection, vulnerability scanning and system monitoring, and miscellaneous technical support for the NRC. The ITI system includes information up to and including Sensitive Unclassified Non-Safeguards Information (SUNSI). Classified and Safeguards Information (SGI) are not permitted on the ITI.
Hearing Audio and Video Equipment System (HAVES)	HAVES is owned by the Atomic Safety and Licensing Board Panel (ASLBP) and uses audio visual technology to support regulatory, licensing, and enforcement processes for adjudicatory hearings on civilian nuclear matters.
Automated Access Control and Computer Enhanced Security System (ACCESS)	ACCESS is a GSS that ensures the physical safety and security of personnel, property, information, infrastructure, and assets. ACCESS encompasses Physical Access Control, Closed-Circuit Television, Intrusion Detection, Heating, Ventilation and Air Conditioning (HVAC) and Lighting systems.

Sources: NRC ITI, HAVES and ACCESS System Security Plans

The audit also included an evaluation of whether the NRC took corrective actions to address open recommendations from the FY 2023 FISMA audit,[23] FY 2022 FISMA audit,[24] FY 2021 FISMA evaluation,[25] FY 2020 FISMA evaluation,[26] and FY 2019 FISMA evaluation.[27] Audit fieldwork was performed from January through June 2024. The audit covered the period from October 1, 2023, through June 30, 2024.

Methodology

To accomplish our objective, we completed the following procedures:

- Evaluated key components of the NRC's information security program and practices, consistent with FISMA and reporting instructions that the OMB and the DHS issued for FY 2024.
- Focused our testing activities on assessing the maturity of the 20 core and 17 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Inquired of NRC management and staff.
- Considered guidance contained in OMB's Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, when planning and conducting our work.
- Evaluated select security processes and controls at the program level, as well as for a non-statistical sample of 3 out of 15 information systems in the NRC's FISMA reportable system inventory. The ITI, HAVES and ACCESS systems are each agency-owned, moderate-impact systems, based on NIST Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information System*.
- Analyzed the ITI, HAVES and ACCESS systems, including reviewing selected system documentation and other relevant information, as well as testing selected security controls to support the IG FISMA Reporting Metrics.
- Reviewed the status of prior-year FISMA recommendations. See **Appendix C** for the status of the prior-year recommendations.

The FY 2023 IG FISMA Reporting Metrics introduced a calculated average scoring model that was continued for the FY 2024 FISMA audit. As part of this approach, IGs must average the ratings for core and supplemental IG FISMA Reporting Metrics independently to determine a domain's maturity level and provide data points for the assessed effectiveness of the program and function. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, calculated averages were not automatically

[23] *Audit of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023* (Report No. OIG-23-A-10, issued September 29, 2023) and *NRC's Vulnerability Assessment and External Penetration Test* (Report No. OIG-23-A-11, issued September 29, 2023).
[24] *Audit of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022* (Report No. OIG-22-A-14, issued September 29, 2022).
[25] *Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2021* (Report No. OIG-22-A-04, issued December 20, 2021).
[26] *Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020* (Report No. OIG-21-A-05, issued March 19, 2021).
[27] *Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2019* (Report No. OIG-20-A-06, issued April 29, 2020).

rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, the OMB strongly encouraged IGs to focus on the results of the core IG FISMA Reporting Metrics, as these tie directly to administration priorities and other high-risk areas. The OMB recommended that IGs use the calculated averages of the supplemental IG FISMA Reporting Metrics as a data point to support their risk-based determination of the overall effectiveness of the program and function.

We used the FY 2024 IG FISMA Reporting Metrics guidance[28] to form our conclusions for each Cybersecurity Framework domain and function, as well as for the overall agency rating. Specifically, we focused on the calculated average scores of the core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average scores of the supplemental IG FISMA Reporting Metrics and progress that the NRC has made in addressing outstanding prior-year recommendations, to form our risk-based conclusion.

We evaluated the effectiveness of the NRC's information security program and practices, including with FISMA and related information security policies, procedures, standards, and guidelines, and responded to the FY 2024 IG FISMA Reporting Metrics. Our work did not include assessing the sufficiency of internal controls over the NRC's information security program or other matters not specifically outlined in this report.

[28] The FY 2024 IG FISMA Reporting Metrics provided the agency IG with the discretion to determine the rating for each of the Cybersecurity Framework domains and functions and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FISMA audit. Using this approach, IGs may determine that a particular domain, function area, or agency's information security program is effective at a calculated maturity level lower than level 4.

APPENDIX C: STATUS OF PRIOR-YEAR RECOMMENDATIONS

Table 5 summarizes the status of the open prior-year recommendations from the FY 2023 FISMA audit, FY 2022 FISMA audit, FY 2021 FISMA evaluation, FY 2020 FISMA evaluation, and FY 2019 FISMA evaluation.[29] At the time of testing and IG FISMA Reporting Metric submission, 21 of the 40 prior-year recommendations from the audits and evaluations referenced above remained open.

The NRC issued memoranda on the *Status of NRC Open Audit Recommendations* (based on audit year) to the NRC OIG demonstrating its progress in remediating the audit recommendations. The "NRC's Status" column of the following table summarizes these memoranda. The "Auditor's Position on Status" column is based on our inspection of evidence received during fieldwork. The auditors will follow up on the open prior-year recommendations recorded in this report during the next audit cycle or through the OIG's status of recommendations process. Additionally, **Table 5** maps the prior-year recommendations to the affected IG FISMA Reporting Metric domains.

Table 5: Prior-Year Recommendations

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
OIG-23-A-10 FY 2023 FISMA Audit **Recommendation 1**	We recommend that NRC management reviews all ITI POA&Ms to ensure that they are accurate and contain detailed information on the status of corrective actions, including changes to scheduled completion dates.	This recommendation remains open. Estimated target completion date: FY 2025 Quarter (Q) 2 NRC management indicated that efforts to develop and implement the required enhancements to NRC's Risk and Continuous Authorization Tracking System (RCATS) tool remain ongoing.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Risk Management**
OIG-23-A-10 FY 2023 FISMA Audit **Recommendation 3**	We recommend that NRC management increases the current Security Information and Event Management (SIEM) tool licensing level and acquires funding to adequately support the procurement, onboarding, and implementation of requirements across all event logging (EL) maturity tiers to ensure events	This recommendation remains open. Estimated target completion date: FY 2025 Q4 NRC management has increased the current SIEM tool licensing level and acquired funding. NRC	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Identity and Access Management** **Incident Response**

[29] See footnotes 22 through 26.

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	are logged and tracked in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).	management plans to implement all requirements across EL maturity tiers EL1, EL2 and EL3 to ensure events are logged and tracked in accordance with OMB M-21-31 by FY 2025 Q4.		
OIG-23-A-11 FY 2023 FISMA Audit Vulnerability and External Penetration Test **Recommendation 1**	Implement corrective actions to address vulnerabilities identified in this report.	This recommendation remains open. Estimated target completion date: FY 2024 Q4 NRC management indicated they will implement corrective actions and document / describe mitigations to address the vulnerabilities identified as part of the FY 2023 FISMA Audit Vulnerability and External Penetration Test by FY 2024 Q4.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Configuration Management**
OIG-23-A-11 FY 2023 FISMA Audit Vulnerability and External Penetration Test **Recommendation 2**	Improve the patch and vulnerability management program to patch security deficiencies within the NRC's defined patching time frame (30 calendar days from identification for Critical and High vulnerabilities).	This recommendation remains open. Estimated target completion date: FY 2024 Q4 NRC management plans to update the patching timeframe policy to align with Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* dated November 3, 2021, and the Cybersecurity and Infrastructure Security Agency's Agency Wide Adaptive Risk Enumeration risk scoring methodology.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing. In addition, current year testing results found that the NRC has open POA&Ms related to configuration settings, least functionality and flaw remediation requirements.	**Configuration Management**
OIG-22-A-14 FY 2022 FISMA Audit	Review and update the ITI Core Services System Security Plan (SSP) System Interconnections tab and	The NRC has reviewed and updated the ITI Core Services SSP System Interconnections	Closed	**Risk Management**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 1	related security control implementation to ensure system interconnection details reflect the current system environment.	tab and related security control implementation details. The NRC requests closure of this recommendation.	The OIG reviewed the ITI Core Services SSP to verify that system interconnection details reflect the current system environment.	**Information Security Continuous Monitoring**
OIG-22-A-14 FY 2022 FISMA Audit **Recommendation 2**	Implement a process to verify that remaining external interconnections noted in the ITI Core Services SSP have documented, up-to-date Interconnection Security Agreements / Memoranda of Understanding or Service Level Agreements in place as applicable.	This recommendation remains open. Estimated target completion date: FY 2024 Q3. The NRC will conduct a training session during its next agencywide Information Systems Security Manager Forum, addressing annual SSP review and update requirements of Computer Security Process (CSO-PROS)-2030 *Risk Management Framework Process* and CSO-PROS-1323 *Continuous Monitoring Process*.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Risk Management**
OIG-22-A-14 FY 2022 FISMA Audit **Recommendation 3**	Update the ITI inventory to correct any discrepancies and incorrect information listed for ITI devices tracked in the Common Computing Services, Peripherals, Unified Communications and Voice over Internet Protocol subsystem inventories.	The NRC has updated the Common Computing Services, Peripherals, Unified Communications and Voice over Internet Protocol subsystem inventories. NRC requests closure of this recommendation.	Closed OIG inspected the ITI inventory to verify ITI inventory detail was updated and has corrected any discrepancies and incorrect information identified for ITI assets in the Common Computing Services, Peripherals, Unified Communications and Voice over Internet Protocol subsystem inventories.	**Risk Management**
OIG-22-A-14 FY 2022 FISMA Audit **Recommendation 4**	Document and implement a periodic review of subsystem inventories to verify information maintained for each ITI subsystem is current, complete, and accurate.	This recommendation remains open. Estimated target completion date: FY 2024 Q4. NRC management indicated that Service area role information technology asset inventory	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Risk Management**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
		responsibilities will be defined, and metrics developed to ensure accuracy. Due to competing priorities and dependencies on a legacy system migration, the NRC's new target completion date is FY 2024 Q4.		
OIG-22-A-14 FY 2022 FISMA Audit **Recommendation 5**	Implement a process to document the supply chain risk management requirements within the NRC information systems' system security plans.	NRC management indicated they have implemented a process to document supply chain risk management requirements within SSPs for their information systems. NRC requests closure of this recommendation.	Closed The OIG reviewed and confirmed that the NRC has updated its organization-defined values for NIST SP 800-53, Revision 5, controls to incorporate supply chain risk management requirements within system security plans for all information systems.	**Supply Chain Risk Management**
OIG-22-A-14 FY 2022 FISMA Audit **Recommendation 6**	Implement a process to validate that all personnel with privileged level responsibilities complete annual security awareness and role-based training.	This recommendation remains open. Estimated target completion date: FY 2024 Q3. NRC management indicated they will implement a process to ensure that all personnel with privileged level responsibilities complete required training as applicable.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Security Training**
OIG-22-A-14 FY 2022 FISMA Audit **Recommendation 7**	Implement a process to validate that all new contractors complete their initial security training requirements and acknowledgement of rules of behavior prior to accessing the NRC environment and to subsequently ensure completion of annual security awareness training and renewal of rules of behavior is tracked.	This recommendation remains open. Estimated target completion date: FY 2024 Q3 NRC management indicated they will implement a process to validate initial and annual security training requirements for new contractors are met.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Security Training**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 2**	Continue current Agency's efforts to update the Agency's cybersecurity risk register to (i) aggregate security risks, (ii) normalize cybersecurity information across organizational units, and (iii) prioritize operational risk response.	NRC updated the cybersecurity risk register to aggregate risk, normalize agency-wide cybersecurity information and prioritize risk responses. NRC requests closure of this recommendation.	Closed OIG verified NRC has completed updates to the agency's cybersecurity risk register.	**Risk Management**
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 3**	Update procedures to include assessing the impacts to the organization's Information Security Architecture (ISA) prior to introducing new information systems or major system changes into the Agency's environment.	At the system level, NRC conducts an impact assessment when new information systems or major changes occur to ensure that they meet the requirements of the agency's cybersecurity and privacy programs. NRC requests closure of this recommendation.	Closed OIG verified impact assessments are generally done at a system level with consideration given to the ISA, if applicable.	**Risk Management**
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 4**	Develop and implement procedures in the POA&M process to include mechanisms for prioritizing completion and incorporating this as part of documenting a justification and approval for delayed POA&Ms.	NRC has developed and implemented CSO-PROS-1701, *Plan of Action and Milestones Prioritization Process*. NRC requests closure of this recommendation.	Closed OIG verified RCATS is used to manage the status and assignment of POA&Ms. OIG also inspected CSO-PROS-2030 and CSO-PROS-1701 to determine they govern POA&M prioritization and management.	**Risk Management**
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 6**	Document and implement policies and procedures for prioritizing externally provided systems and services or a risk-based process for evaluating cyber supply chain risks associated with third party providers.	This recommendation remains open. Estimated target completion date: FY 2024 Q3 NRC will finalize the two draft CSO-PROS being actively used to assess supply chain risk associated with an ICT product or service, perform appropriate responsive actions, and monitor the risk over time once enough assessments have been performed to determine the effectiveness of the evaluations.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Supply Chain Risk Management**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 7**	Implement processes for continuous monitoring and scanning of counterfeit components to include configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.	This recommendation remains open. Estimated target completion date: FY 2025 Q1 The NRC will update CSO-PROS-0006 *Counterfeit and Compromised ICT Product Detection Process* to include the vetting of third-party service personnel and replacement parts to detect counterfeit parts and other components from being added to its environment.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Supply Chain Risk Management**
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 8**	Develop and implement role-based training with those who hold supply chain risk management roles and responsibilities to detect counterfeit system components.	This recommendation remains open. Estimated target completion date: FY 2025 Q3 Pursuant to the *Supply Chain Security Training Act of 2021*, Pub. L. 117-145, General Services Administration is required to develop training for federal officials with supply chain risk management responsibilities. NRC will leverage this training, which will be implemented by OMB, when it becomes available.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Supply Chain Risk Management** **Security Training**
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 11**	Update user system access control procedures to include the requirement for individuals to complete a non-disclosure and rules of behavior agreements prior to the individual being granted access to NRC systems and information.	This recommendation remains open. Estimated target completion date: FY 2024 Q3 The NRC will update its onboarding procedures to require individuals to complete a	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Identity and Access Management**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
		nondisclosure agreement before they are granted access to the agency's systems and information.		
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 12**	Conduct an independent review or assessment of the NRC privacy program and use the results of these reviews to periodically update the privacy program.	The NRC has conducted an in-depth, independent assessment of the agency's privacy program. Using the results of the assessment, the NRC will use these reviews to periodically update the privacy program. NRC requests closure of this recommendation.	Closed OIG reviewed and confirmed that the NRC has conducted an in-depth, independent assessment of the agency's privacy program, the results of which will be used for periodic updates, as needed.	**Data Protection and Privacy**
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 13**	Implement the technical capability to restrict access or not allow access to the NRC's systems until new NRC employees and contractors have completed security awareness training and role-based training as applicable or implement the technical capability to capture NRC employees and contractor's initial login date so that the required cybersecurity awareness and role-based training can be accurately tracked and managed by the current process in place.	This recommendation remains open. Estimated target completion date: FY 2025 Q3 The NRC plans to add streamlined security training that contains the Rules of Behavior but does not contain sensitive information to its onboarding process, which occurs before employees and contractors gain access to the NRC network. The agency will also strengthen its post-onboarding process to ensure that new employees and contractors complete all required security awareness and role-based training, including acknowledging the Rules of Behavior, within the required timeframe.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Security Training**
OIG-22-A-04 FY 2021 FISMA Evaluation	Implement the technical capability to restrict NRC network access for employees who do not complete annual security awareness training	This recommendation remains open. Estimated target completion date: FY 2024 Q3	Closed We noted this recommendation was a duplicate of Recommendation 8 in OIG-21-05	**Security Training**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 14	and, if applicable, their assigned role-based security training.	NRC Office of Chief Information Officer staff will consult with stakeholders to develop a specific, risk-based solution to restrict NRC network access for employees who do not complete required training.	(FY 2020 FISMA Evaluation); therefore, we have closed this recommendation.	
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 16**	Conduct an organizational level BIA to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.	This recommendation remains open. Estimated target completion date: FY 2024 Q3 NRC will conduct an organizational level BIA.	Closed We noted this recommendation was a duplicate of Recommendation 10 in OIG-21-05 (FY 2020 FISMA Evaluation); therefore, we have closed this recommendation.	**Contingency Planning**
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 17**	Integrate metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency plans, as appropriate, to deliver persistent situational awareness across the organization.	This recommendation remains open. Estimated target completion date: FY 2024 Q4 NRC will integrate contingency planning metrics with other related plans, as appropriate, to deliver persistent situation awareness across the agency.	Closed We noted this recommendation was a duplicate of Recommendation 12 in OIG-21-05 (FY 2020 FISMA Evaluation); therefore, we have closed this recommendation.	**Contingency Planning**
OIG-22-A-04 FY 2021 FISMA Evaluation **Recommendation 18**	Update and implement procedures to coordinate contingency plan testing with ICT supply chain providers.	This recommendation remains open. Estimated target completion date: FY 2024 Q4 The NRC is assessing approaches to implement procedures to coordinate contingency plan testing with ICT supply chain providers.	Closed We noted this recommendation was a duplicate of Recommendation 13 in OIG-21-05 (FY 2020 FISMA Evaluation); therefore, we have closed this recommendation.	**Supply Chain Risk Management** **Contingency Planning**
OIG-21-A-05 FY 2020 FISMA Evaluation	If necessary, update enterprise, business process, and information system level risk tolerance and	The NRC has transitioned all FISMA system security plans to NIST SP 800-53 Revision 5	Closed	**Risk Management**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 2(c)	appetite levels necessary for prioritizing and guiding risk management decisions.	requirements and enhanced the POA&M prioritization process through migration of all FISMA systems to RCATS for POA&M management. The NRC has also updated risk tolerance and appetite levels at the enterprise, business process and information system levels, as necessary.	OIG reviewed and confirmed that the NRC's work related to the RCATS POA&M prioritization process and Risk Management Process satisfy the recommendation to update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.	
OIG-21-A-05 FY 2020 FISMA Evaluation **Recommendation 2(e)**	Consistently assess the criticality of POA&Ms to support why a POA&M is or is not of a high or moderate impact to the Confidentiality, Integrity and Availability of the information system, data, and mission.	NRC has completed efforts to migrate all FISMA systems to RCATS. The completion of this effort, in combination with applicable CSO-PROS helps with consistently assessing the criticality of POA&Ms.	Closed OIG reviewed and confirmed that the NRC's POA&Ms are consistently assessed to support why a POA&M is or is not high or moderate impact to the Confidentiality, Integrity and Availability of the information system, data, and mission.	**Risk Management**
OIG-21-A-05 FY 2020 FISMA Evaluation **Recommendation 5**	Update user system access control procedures to include the requirement for individuals to complete a non-disclosure agreement as part of the clearance waiver process prior to the individual being granted access to the NRC systems and information. Also, incorporate the requirement for contractors and employees to complete non-disclosure agreements as part of the agency's on-boarding procedures prior to these individuals being granted access to the NRC's systems and information.	This recommendation remains open. Estimated target completion date: FY 2025 Q3 The NRC will update its onboarding procedures to require individuals to complete a nondisclosure agreement before they are granted access to the NRC's systems and information.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Identity and Access Management**
OIG-21-A-05 FY 2020 FISMA Evaluation	Continue efforts to identify individuals having additional responsibilities for PII or activities involving PII and	This recommendation remains open.	Open We inspected the documentation provided in response to our follow-	**Data Protection and Privacy**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 6	develop role-based privacy training for them to be completed annually.	Estimated target completion date: FY 2025 Q2 The NRC has identified individuals with privacy roles and will develop role-based privacy training through modification to existing training courses and/or development of new training, as necessary.	up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	
OIG-21-A-05 FY 2020 FISMA Evaluation **Recommendation 8**	Implement the technical capability to restrict NRC network access for employees who do not complete annual security awareness training and, if applicable, their assigned role-based security training.	This recommendation remains open. Estimated target completion date: FY 2025 Q3 NRC Office of Chief Information Officer staff will consult with stakeholders to develop a specific, risk-based solution to restrict NRC network access for employees who do not complete required training.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Security Training**
OIG-21-A-05 FY 2020 FISMA Evaluation **Recommendation 10**	Conduct an organizational level BIA to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.	NRC has done an organizational level BIA.	Closed We inspected the organization level BIA conducted by the agency to verify the NRC has determined and documented their contingency planning requirements and priorities, including for mission essential functions and high value assets, making updates to contingency planning policies and procedures as necessary (e.g., continuity of operations plan and related training).	**Contingency Planning**
OIG-21-A-05 FY 2020 FISMA Evaluation	Integrate metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans,	This recommendation remains open.	Open We inspected the documentation provided in response to our follow-	**Contingency Planning**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 12	such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency plans, as appropriate, to deliver persistent situational awareness across the organization.	Estimated target completion date: FY 2025 Q4 NRC will analyze its contingency plans to identify opportunities to integrate metrics for measuring the effectiveness of the associated information system.	up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	
OIG-21-A-05 FY 2020 FISMA Evaluation **Recommendation 13**	Implement automated mechanisms to test system contingency plans, then update and implement procedures to coordinate contingency plan testing with ICT supply chain providers and implement an automated mechanism to test system contingency plans.	This recommendation remains open. Estimated target completion date: FY 2025 Q2 NRC will analyze its contingency plans to identify candidates for automated testing. Based on that analysis, if automated testing is feasible and cost effective, then the NRC will develop plans to implement those measures and coordinate with all associated ICT supply chain providers.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Supply Chain Risk Management** **Contingency Planning**
OIG-20-A-06 FY 2019 FISMA Evaluation **Recommendation 2(c)**	Use the fully defined ISA to formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.	This recommendation remains open. Estimated target completion date: FY 2024 Q4 NRC has transitioned and assessed eight of its 15 information systems to NIST SP 800-53, Revision 5. The agency expects to complete the transition and assessment of the remaining 7 systems by FY 2024 Q4.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Risk Management**
OIG-20-A-06 FY 2019 FISMA Evaluation	Use the fully defined ISA to conduct an organization-wide security and privacy risk assessment.	NRC used its fully defined ISA to conduct an organization	Closed	**Risk Management**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 2(d)		wide security risk assessment, as well as an assessment of privacy risks. NRC requests closure of this recommendation.	OIG confirmed that the NRC has used the fully defined ISA to conduct an organization-wide security and privacy risk assessment. OIG also noted the assessments are performed in a three-cycle review process covering all five NIST Cybersecurity Framework functions.	
OIG-20-A-06 FY 2019 FISMA Evaluation **Recommendation 2(e)**	Use the fully defined ISA to conduct a supply chain risk assessment.	NRC used its fully defined ISA to conduct a supply chain risk assessment. NRC requests closure of this recommendation.	Closed OIG confirmed that the NRC has used the fully defined ISA to conduct a supply chain risk assessment.	**Supply Chain Risk Management**
OIG-20-A-06 FY 2019 FISMA Evaluation **Recommendation 2(f)**	Use the fully defined ISA to identify and update NRC risk management policies, procedures, and strategy.	Based on the fully defined ISA, the NRC evaluated its cybersecurity policy and risk management strategy and made updates if necessary. NRC requests closure of this recommendation.	Closed OIG confirmed the NRC has used its fully defined ISA to identify and update the NRC Risk Management Framework process.	**Risk Management** **Information Security Continuous Monitoring**
OIG-20-A-06 FY 2019 FISMA Evaluation **Recommendation 4**	Perform an assessment of role-based privacy training gaps.	The NRC performed an assessment of role-based privacy training gaps in October 2023. As a result of the assessment, the NRC will identify individuals having specialized role-based responsibilities for PII or activities involving PII and develop role-based privacy training for them. NRC requests closure of this recommendation.	Closed OIG confirmed that the NRC had performed an assessment of the role-based privacy training gaps.	**Data Protection and Privacy**
OIG-20-A-06 FY 2019 FISMA Evaluation **Recommendation 5**	Identify individuals having specialized role-based responsibilities for PII or activities involving PII and develop role-based privacy training for them.	This recommendation remains open. Estimated target completion date: FY 2025 Q1	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and	**Data Protection and Privacy**

Report No. Recommendation No.	Recommendation	NRC's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
		Based on the results of the assessment referenced in recommendation 4 above, the NRC will update and develop annual role-based privacy training. The assessment is scheduled to be completed in Q2 of FY 2024. The agency plans to complete the associated training development and implementation by FY 2025, Q1.	determined that corrective action is ongoing.	
OIG-20-A-06 FY 2019 FISMA Evaluation **Recommendation 6**	Based on NRC's supply chain risk assessment results, complete updates to the NRC's contingency planning policies and procedures to address supply chain risk training for them.	This recommendation remains open. Estimated target completion date: FY 2025 Q1 The NRC estimates that the agency will need six months to complete this task after resolution of recommendation 2e above.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Supply Chain Risk Management** **Contingency Planning**
OIG-20-A-06 FY 2019 FISMA Evaluation **Recommendation 7**	Continue efforts to conduct agency and system level business impact assessments to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.	This recommendation remains open. Estimated target completion date: FY 2024 Q4 NRC conducts system level BIAs and plans to conduct an agency (i.e., organizational) level BIA.	Closed. We inspected the organization level BIA conducted by the agency to verify the NRC has determined and documented their contingency planning requirements and priorities, including for mission essential functions and high value assets, making updates to contingency planning policies and procedures as necessary (e.g., continuity of operations plan and related training).	**Contingency Planning**

APPENDIX D: MANAGEMENT RESPONSE

The OIG and Sikich held an exit conference with the agency on September 16, 2024. Before the exit conference, agency management reviewed and provided editorial comments on the discussion draft version of this report, and the OIG and Sikich discussed these comments with the agency during the conference. Sikich has incorporated the agency's comments into this report as appropriate. NRC management chose not to provide formal comments for inclusion in this report. Responsible officials will provide agency planned corrective actions within 30 days following report publication as part of the audit resolution process.