MEMORANDUM

DATE: September 29, 2023

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 (OIG-23-A-10)

The Office of the Inspector General (OIG) contracted with CliftonLarsonAllen LLP (CLA) to conduct the *Audit of the U.S. Nuclear Regulatory Commission's (NRC) Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023*. 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 NRC. 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. Following the exit conference, the agency's staff indicated that they had no formal comments for inclusion in this report.

For the period October 1, 2022, through June 30, 2023, CLA found that although the NRC established an effective agency-wide information security program and practices, there are weaknesses that may have some impact on the agency's ability to optimally protect the NRC's systems and information.

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 Terri Cooper, Team Leader, at 301.415.5965.

Attachment:
As stated

cc: M. Bailey, AO
M. Meyer, DAO
J. Jolicoeur, OEDO
OIG Liaison Resource
EDO_ACS Distribution

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

Fiscal Year 2023

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) information security program and practices for fiscal year (FY) 2023 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The 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 objective of this performance audit was to assess the effectiveness of the information security policies, procedures, and practices of the NRC.

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.

For this year's review, IGs were required to assess 20 Core IG FISMA Reporting Metrics and 20 Supplemental IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area.[1] 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, the NRC's information security program must be rated Level 4 – *Managed and Measurable*.

The audit included an assessment of the NRC's information security programs and practices consistent with the FISMA and reporting instructions issued by the Office of Management and Budget (OMB). The scope also included assessing selected security controls outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for a sample of systems in the NRC's FISMA inventory of information systems. Audit fieldwork covered the NRC's headquarters located in Rockville, MD from January 2023 to June 2023. The audit covered the period from October 1, 2022, through June 30, 2023.

We concluded that the NRC implemented effective information security policies, procedures, and practices, since it achieved an overall *Level 4 – Managed and Measurable* maturity level; therefore, the NRC has an effective information security program. Although we concluded that the NRC implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted new and repeat weaknesses in its security program related to the risk management, supply chain risk management, configuration management, identity and access management, security training, incident response, and contingency planning domains of the FY 2023 IG FISMA Reporting Metrics. As a result, we made three new recommendations to assist the NRC in strengthening its information security program. Additionally, we noted 21 prior year recommendations remain open from the FY 2022 FISMA audit and FY 2021 FISMA evaluation based on inspection of evidence received during fieldwork.

[1] The function areas are further broken down into nine domains.

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 13, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 13, 2023.

The purpose of this audit report is to report on our assessment of the NRC's compliance with the FISMA 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
September 13, 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. The 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 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 information security policies, procedures, and practices of the NRC.

The OMB and the Department of Homeland Security (DHS) annually provide instructions to federal agencies and IGs for preparing FISMA reports. On December 2, 2022, the OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*.[2] According to that memorandum, each year the IGs are required to complete IG FISMA Reporting Metrics[3] to independently assess their agencies' information security program. The OMB selected a core group of metrics[4] that Inspectors General must evaluate annually and a selection of 20 Supplemental IG FISMA Reporting Metrics that must be evaluated during FY 2023.[5] The remainder of standards and controls will be evaluated on a two-year cycle.

For this year's review, IGs were required to assess 20 Core IG FISMA Reporting Metrics and 20 Supplemental IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area.[6] 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 I** for additional information on the FISMA reporting requirements.

The audit included an assessment of the NRC's information security program and practices consistent with the FISMA and reporting instructions issued by the OMB. In addition, we reviewed selected controls from NIST Special Publication (SP) 800-53,

[2] See OMB M-23-03 online here.
[3] See FY 2023 – FY 2024 IG FISMA Reporting Metrics online here. We submitted our responses to the FY 2023 IG FISMA Reporting Metrics to NRC OIG as a separate deliverable under the contract for this audit.
[4] Core Metrics represent a combination of Administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.
[5] Supplemental Metrics represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.
[6] The function areas are further broken down into nine domains.

Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2023 IG FISMA Reporting Metrics for a sample of three of 15 information systems[7] in the NRC's FISMA inventory of information systems as of January 2023.[8] The scope also included an independent vulnerability assessment and external penetration test (technical assessment) of the NRC headquarters network.[9]

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 implemented effective information security policies, procedures, and practices, since it achieved an overall *Level 4 – Managed and Measurable* maturity level; therefore, the NRC has an effective information security program.[10] For example, the NRC:

- Maintained an effective continuous monitoring program including periodic security control assessments and dashboards for tracking risk management posture.
- Integrated the privacy program with other security areas and business processes as well as embedded the privacy program into daily decision making to help identify and manage privacy risks.
- Maintained an effective incident response program.

Table 1 below shows a summary of the overall assessed maturity levels for each function area and domain in the FY 2023 IG FISMA Reporting Metrics.

Table 1: Maturity Levels for FY 2023 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Maturity Level by Function	Metric Domains	Maturity Level by Domain
Identify	Level 4: Managed and Measurable	**Risk Management**	Level 4: Managed and Measurable
		Supply Chain Risk Management	Level 3: Consistently Implemented
Protect	Level 4: Managed and Measurable	**Configuration Management**	Level 4: Managed and Measurable

[7] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
[8] NRC's FISMA inventory of information systems details a list of NRC's FISMA reportable systems.
[9] Detailed results of the technical assessment are presented in a separate report under limited distribution due to the sensitive nature of the results.
[10] In the FY 2022 FISMA audit, the results were based on the 20 metric questions. The FY 2023 FISMA audit results are based on 40 metric questions.

Cybersecurity Framework Security Functions	Maturity Level by Function	Metric Domains	Maturity Level by Domain
		Identity and Access Management	Level 4: Managed and Measurable
		Data Protection and Privacy	Level 5: Optimized
		Security Training	Level 3: Consistently Implemented
Detect	Level 4: Managed and Measurable	**Information Security Continuous Monitoring**	Level 4: Managed and Measurable
Respond	Level 4: Managed and Measurable	**Incident Response**	Level 4: Managed and Measurable
Recover	Level 3: Consistently Implemented	**Contingency Planning**	Level 3: Consistently Implemented
Overall	**Level 4: Managed and Measurable – Effective**		

Although we concluded that the NRC implemented an effective information security program, overall, its implementation of a subset of selected controls was not fully effective. We noted new and repeat weaknesses in its security program related to risk management, supply chain risk management, configuration management, identity and access management, security training, incident response, and contingency planning domains of the FY 2023 IG FISMA Reporting Metrics (see **Table 2** below).

As a result of the weaknesses noted, we made three new recommendations to assist the NRC in strengthening its information security program. Additionally, we noted 21 prior year recommendations remain open from the FY 2022 FISMA audit and FY 2021 FISMA evaluation based on inspection of evidence received during fieldwork.[11] **Table 2** also includes weaknesses where the NRC has prior year recommendations that remain open related to the FY 2023 IG FISMA Reporting Metrics.

[11] See appendix III for status of prior year recommendations.

Table 2: Weaknesses Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2023 IG FISMA Reporting Metrics

Cybersecurity Framework Security Function	FY 2023 IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	Weaknesses in the NRC's Plan of Action and Milestones (POA&M) Management Process **(Finding 1)**.
	Supply Chain Risk Management	Open prior year recommendations related to documenting supply chain risk management in all system security plans.[12]
Protect	**Configuration Management**	Weaknesses in the NRC's Vulnerability Management Program **(Finding 2)**.
	Identity and Access Management	Weakness in the NRC's Inactive Account Management **(Finding 3).** Open prior year recommendations related to completing access agreements before granting access.
	Data Protection and Privacy	No weaknesses noted.
	Security Training	Open prior year recommendations related to completion of security awareness and role-based training.
Detect	**Information Security Continuous Monitoring**	No weaknesses noted.
Respond	**Incident Response**	Weaknesses in the NRC's Event Logging Maturity **(Finding 4)**.
Recover	**Contingency Planning**	Open prior year recommendations related to organization level business impact analysis and contingency plan testing integration with information and communications technology (ICT) supply chain providers.

The following sections provide a detailed discussion of the audit findings. **Appendix I** provides background information on the FISMA. **Appendix II** describes the audit objective, scope, and methodology. **Appendix III** provides the status of the prior years' recommendations.

[12] See appendix III for the status of the prior years' open recommendations.

AUDIT FINDINGS

1. Weaknesses in the NRC's Plan of Action and Milestones (POA&M) Management Process

Cybersecurity Framework Security Function: *Identify*
FY 2023 IG FISMA Reporting Metrics Domain: *Risk Management*

We noted 686 of 4,775 open Information Technology Infrastructure (ITI) system POA&Ms did not have current milestone dates to meet their updated scheduled completed dates.

Updates to POA&Ms rely on active communication with System Administrators and other parties, which falters in some cases.

NRC's Computer Security Organization (CSO)-Computer Security Process (PROS)-2016, *Plan of Action and Milestones Process*, Section 3.4, states,

> "POA&Ms must be reviewed and maintained at least quarterly by system ISSOs or CSO program level assigned resource to ensure that identified milestones are completed by the scheduled completion dates. In addition, POA&Ms must be updated whenever activities take place that either identify new weaknesses, demonstrate that weaknesses have been remediated, extend the schedule for remediation, or demonstrate that required continuous monitoring activities have been completed. Before each quarterly review, system ISSOs or the CSO program level assigned resource must review their POA&Ms to ensure that the following information is up-to-date and reflects all corrective actions that took place during the previous quarter."

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, security control CA-5 – Plan of Action and Milestones, states:

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and,
b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Without timely completion of ITI POA&Ms, the NRC ITI subsystems and other information systems that rely on ITI security controls through inheritance or hybrid implementations could remain susceptible to significant system security risks. In addition, without sufficient information about the ongoing status of open ITI POA&Ms, the NRC may not accurately know and have full visibility into the status of vulnerabilities and risks on their systems.

> ***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.*

2. Weaknesses in the NRC's Vulnerability Management Program

Cybersecurity Framework Security Function: *Protect*
FY 2023 IG FISMA Reporting Metrics Domain: *Configuration Management*

The scope of the FY 2023 FISMA audit included an independent vulnerability assessment and external penetration test (technical assessment) performed under executed rules of engagement in accordance with NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*. The technical assessment noted that a vulnerability management process and procedures have been established. However, the NRC's implementation of certain vulnerability management program requirements was not fully achieved with regards to remediation timeframes established by NRC's policy. For more information, please refer to the restricted FY 2023 Vulnerability Assessment and External Penetration Test Results Memo with limited distribution due to the sensitive nature of the results.

This finding is included as a reference within this report since the Configuration Management domain and vulnerability management related controls of the IG FISMA Reporting Metrics are within the scope of the FY 2023 FISMA audit.

NRC OIG intends to follow-up on NRC management's corrective actions taken as part of the FY 2024 FISMA audit of NRC's information security program and practices.

3. Weaknesses in the NRC's Inactive Account Management

Cybersecurity Framework Security Function: *Protect*
FY 2023 IG FISMA Reporting Metrics Domain: *Identity and Access Management*

The ITI Core Services[13] 90-day account disablement script was not consistently capturing all inactive accounts. Specifically, we noted that ITI Core Services had nine (9) non-privileged and twenty-four (24) privileged Active Directory users with active accounts that were inactive for more than 90-days.

NRC management indicated the ITI Core Services 90-day account disablement script was not configured to capture and disable certain Active Directory 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].

[13] ITI Core Services is a subsystem of ITI that includes Microsoft's Active Directory.

Without a consistent script to disable all inactive or otherwise unnecessary Active Directory accounts, there is a greater potential risk of individuals gaining unauthorized access to the NRC network environment.

> ***Recommendation 2:*** *We recommend NRC management implement a revised ITI Core Services 90-day account disablement script to ensure all non-privileged and privileged Active Directory accounts are captured and disabled in accordance with NRC policies.*
>
> *After notification of the audit finding, NRC management implemented a revised ITI Core Services 90-day account disablement script. The effectiveness of the revised script will be assessed during the next audit period.*

4. Weaknesses in the NRC's Event Logging Maturity

Cybersecurity Framework Security Function: *Respond*
FY 2023 IG FISMA Reporting Metrics Domain: *Incident Response*

The NRC assessed their Event Logging (EL) maturity against the requirements in the Office of Management and Budget (OMB) Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021), and reported their current EL maturity level as EL0, [14] not-effective.

While the NRC is developing a plan to assist with reaching compliance with OMB M-21-31 requirements, the NRC did not reach EL1[15] and EL2[16] maturity levels by OMB's required due dates. Specifically, the NRC did not:

- Within one year of the date of OMB M-21-31, or by August 27, 2022, reach EL1 maturity level.
- Within 18 months of the date of OMB M-21-31, or by February 27, 2023, achieve EL2 maturity level.

Further, the NRC did not document any risk-based decisions, including compensating controls, for not meeting the requirements in OMB M-21-31.

NRC management indicated that they were constrained by their current Security Information and Event Management (SIEM) tool licensing level and unavailability of funding to adequately support the procurement, onboarding, and implementation of EL1 and EL2 maturity level requirements by the required deadlines.

OMB M-21-31 addresses the logging requirements in the Executive Order 14028, *Improving the Nation's Cybersecurity*[17] (May 12, 2021). OMB M-21-31 establishes a maturity model to guide the implementation of requirements across EL tiers as shown below that are designed to help agencies prioritize their efforts and resources to achieve

---

[14] Per OMB M-21-31, EL0 maturity level signifies logging requirements of highest criticality are either not met or are only partially met. See OMB M-22-18 online here.
[15] Per OMB M-21-31, EL1 maturity level signifies only logging requirements of highest criticality are met.
[16] Per OMB M-21-31, EL2 maturity level signifies logging requirements of highest and intermediate criticality are met.
[17] See Executive Order 14028 online here.

full compliance with requirements for implementation, log categories, and centralized access. OMB M-21-31 further requires that agencies forward all required event logs, in near real-time and on an automated basis, to centralized systems responsible for SIEM.[18]

The maturity model to guide the implementation of requirements is summarized below:

Tier EL0, Rating – Not Effective

The agency or one or more of its components have not implemented the following requirement:

- Ensuring that the Required Logs categorized as Criticality Level 0 are retained in acceptable formats for specified timeframes, per technical details described in OMB M-21-31, Appendix C (Logging Requirements – Technical Details).

Tier EL1, Rating – Basic (to be met by August 27, 2022)

The agency and all of its components meet the following requirements, as detailed in Table 2 (EL1 Basic Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Basic Logging Categories
- Minimum Logging Data
- Time Standard
- Event Forwarding
- Protecting and Validating Log Information
- Passive DNS [Domain Name System]
- Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigations Access Requirements
- Logging Orchestration, Automation, and Response – Planning
- User Behavior Monitoring – Planning
- Basic Centralized Access

Tier EL2, Rating – Intermediate (to be met by February 26, 2023)

The agency and all of its components meet the following requirements, as detailed in Table 3 (EL2 Intermediate Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Meeting EL1 maturity level
- Intermediate Logging Categories
- Publication of Standardized Log Structure
- Inspection of Encrypted Data
- Intermediate Centralized Access

Tier EL3, Rating – Advanced (to be met by August 27, 2023)

[18] SIEM tools are a type of centralized logging software that can facilitate aggregation and consolidation of audit log records from multiple information system components. SIEM tools automate the collection of audit log records from tools and reporting them to a management console in a standardized format and facilitate audit record correlation and analysis.

The agency and all its components meet the following requirements, as detailed in Table 4 (EL3 Advanced Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Meeting EL2 maturity level
- Advanced Logging Categories
- Logging Orchestration, Automation, and Response – Finalizing Implementation
- User Behavior Monitoring – Finalizing Implementation
- Application Container Security, Operations, and Management
- Advanced Centralized Access

Further, OMB M-21-31, Section II: Agency Implementation Requirements, requires agencies to perform the following:

- Within 60 calendar days of the date of OMB M-21-31 [or by October 26, 2021] memorandum, assess their maturity against the maturity model in OMB M-21-31 and identify resourcing and implementation gaps associated with completing each of the requirements listed below. Agencies will provide their plans and estimates to their OMB Resource Management Office and Office of the Federal Chief Information Officer desk officer.
- Within one year of the date of OMB Memorandum 21-31 [or by August 27, 2022], reach EL1 maturity.
- Within 18 months of OMB M-21-31 [or by February 26, 2023], achieve EL2 maturity.
- Within two years of OMB Memorandum 21-31 [or by August 27, 2023], achieve EL3 maturity.
- Provide, upon request and to the extent consistent with applicable law, relevant logs to the CISA and Federal Bureau of Investigations. This sharing of information is critical to defend federal information systems.
- Share log information, as needed and appropriate, with other federal agencies to address cybersecurity risks or incidents.

Cyber-attacks underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud services providers) is invaluable in the detection, investigation, and remediation of cyber threats. By not achieving EL1 and EL2 maturity levels, the NRC is not meeting logging requirements of highest criticality. NRC maturity is currently at EL0 maturity; therefore, their event logging capabilities are not effective based on OMB M-21-31. Further, the NRC may not correlate audit log records across different repositories in a complete or risk-based manner as defined by OMB M-21-31, which may increase the risk that the NRC may not collect all meaningful and relevant data on suspicious events. This may, in turn increase the risk that the NRC may inadvertently miss the potential scope or veracity of suspicious events or attacks.

> ***Recommendation 3:*** *We recommend that NRC management increases the current SIEM tool licensing level and acquires funding to adequately support the procurement, onboarding, and implementation of requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.*

BACKGROUND

Overview

The Energy Reorganization Act of 1974 created the NRC, and the NRC began operations on January 19, 1975. The NRC is headed by a five-member Commission, with one member designated by the President to serve as Chair. 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's broad areas of responsibility include reactor safety oversight and license renewal for existing plants, materials safety oversight and licensing for a variety of purposes, and oversight of the management and disposal of both high-level waste and low-level radioactive waste.

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:[19]

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.
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.

[19] 44 U.S.C. § 3554, Federal agency responsibilities.

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.

National Institute of Standards and Technology (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.

FISMA Reporting Requirements

The OMB and the DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On December 2, 2022, OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*.[20] This memorandum described key changes to the methodology for conducting FISMA audits, as well as the processes for Federal agencies to report to the OMB, and where applicable, the DHS. Key changes to the methodology included:

- The OMB selected a core group of metrics that Inspectors General must evaluate annually and a selection of 20 Supplemental IG FISMA Reporting Metrics that must be evaluated during FY 2023.[21] The remainder of standards and controls will be evaluated on a two-year cycle.
- In previous years, IGs have been directed to utilize a mode-based scoring approach to assess maturity levels. In FY 2023, ratings were focused on calculated averages, wherein the average of the metrics in a particular domain would be used by IGs to determine the effectiveness of individual function areas (Identity, Protect, Detect, Respond, and Recover). IGs were encouraged to focus on the calculated averages of the 20 Core IG FISMA Reporting Metrics, as these tie directly to the Administration's priorities and other high-risk areas. In addition, OMB M-23-03 indicated that IGs should use the calculated averages of the Supplemental IG FISMA Reporting Metrics and progress addressing outstanding prior year recommendations as data points to support their risk-based determination of overall program and function level effectiveness. The calculated averages can be found in the FY 2023 IG FISMA Reporting Metrics, which was provided to the agency separate from this report.

The FY 2023 IG FISMA Reporting Metrics provided the reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.

[20] See OMB M-23-03 online here.
[21] See FY 2023 – FY 2024 IG FISMA Reporting Metrics online here.

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

For this year's review, IGs were to assess the 20 Core IG FISMA Reporting Metrics and 20 Supplemental IG FISMA Reporting Metrics in the five security function areas to assess the maturity level and effectiveness of their agency's information security program. 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 *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover, as highlighted in **Table 3**.

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2023 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Domains in the FY 2023 IG FISMA Reporting Metrics
Identify	Risk Management, Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

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. The table below 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 4: IG Evaluation Maturity Levels

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

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.

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.

For this year's review, IGs were to assess 20 Core IG FISMA Reporting Metrics and 20 Supplemental IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area. The maturity levels range from lowest to highest — Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

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

We utilized the FY 2023 IG FISMA Reporting Metrics guidance[22] to form our conclusions for each Cybersecurity Framework domain, function, and the overall agency rating. Specifically, we focused on the calculated average of the Core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average of the Supplemental IG FISMA Reporting Metrics and progress made addressing outstanding prior year recommendations, to form our risk-based conclusion.

[22] The FY 2023 IG FISMA Reporting Metrics provided the agency IG 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 lower lever than level 4.

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

The scope of this performance audit was to assess the NRC's information security program and practices consistent with the FISMA and reporting instructions issued by the OMB and the DHS for FY 2023. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* mapped to the FY 2023 IG FISMA Reporting Metrics, for a sample of three of 15 information systems in the NRC's FISMA inventory of information systems as of January 4, 2023 **(Table 5)**.

Table 5: Description of System Selected for Testing

System Name	Description
Information Technology Infrastructure (ITI) System	The NRC ITI is a General Support System (GSS) that supports the agency'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.
Agencywide Documents Access and Management System (ADAMS)	ADAMS is used to manage content created by the staff and external stakeholders and is the NRC's official record management system. There is publicly accessible ADAMS and an "inward" facing version that contains documents marked as Official Use Only (OUO).
Business Applications Support System (BASS)	BASS provides a common platform for the operations and maintenance of several NRC applications, including: Reactor Program System (RPS), Operator License Tracking System (OLTS), General License Tracking System (GLTS) and Case Management System Web (CMSW).

In addition, an independent vulnerability assessment and external penetration test was performed under executed rules of engagement prepared in accordance with the NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*. Detailed results of the technical assessment of the NRC's network infrastructure, servers, workstations, applications, and routers accessible internally from the NRC's network and accessible externally from the public Internet are presented in a separate report under limited distribution due to the sensitive nature of the results.

The audit also included an evaluation of whether the NRC took corrective action to address open recommendations from the FY 2022 FISMA audit[23] and FY 2021 FISMA evaluation.[24]

[23] *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).
[24] *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).

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

Audit fieldwork covered the NRC's headquarters located in Rockville, Maryland from January 2023 to June 2023. The audit covered the period from October 1, 2022, through June 30, 2023.

Methodology

To determine if the NRC implemented an effective information security program, we conducted interviews with NRC 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's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, we compared documents, such as the NRC's 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. Finally, we reviewed the status of FISMA prior year recommendations. See Appendix III for the status of prior year recommendations.

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).
- Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).
- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022).
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022).
- CISA's BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities.*
- FY 2023 IG FISMA Reporting Metrics (February 10, 2023).
- 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 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (November 11, 2011).
- 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);*
- *NRC ITI, ADAMS, and BASS System Security Plans (SSPs);*
- *NRC ITI, ADAMS, and BASS Configuration Management Plans;*
- *NRC ITI, ADAMS, and BASS Information System Contingency Plans (ISCPs);*
- *NRC Enterprise Risk Management Plan;*
- *NRC Risk Management Framework Process;*
- *NRC Supply Chain Risk Management Strategy;*
- *NRC Privacy Program Plan;*
- *NRC Computer Security Process (CSO-PROS)-1323 Information Security Continuous Monitoring Process; and*
- *NRC Computer Security Incident Response Team Standard Operating Procedures.*

We selected three NRC information systems from the total population of 15 FISMA reportable systems for testing. The three systems were selected based on risk, date of last evaluation and criticality. Specifically, ITI was selected based on risk since it is categorized as a moderate impact system[25] and supports the NRC's applications that reside on the network. ADAMS was selected because it is categorized as a moderate impact system and was last evaluated in 2019. The third system selected for testing was BASS, a moderate impact system that was last evaluated in 2017. We tested the three systems' selected security controls to support our responses to the FY 2023 IG FISMA Reporting Metrics.

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.

[25] The selected systems were categorized as moderate impact based on NIST Federal Information Processing Standards Publication 199 *Standards for Security Categorization of Federal Information and Information Systems*.

STATUS OF PRIOR RECOMMENDATIONS

The table below summarizes the status of the open prior recommendations from the FY 2022 FISMA audit and FY 2021 FISMA evaluation.[26] At the time of testing and IG FISMA Reporting Metric submission, there remained 21 out of 24 open prior FISMA recommendations from the audit and evaluation referenced above. The NRC OIG gathered feedback from NRC stakeholders in support of Status of Recommendations Memorandums issued March 6, 2023 and February 15, 2023, which are reflected here as part of the NRC's status. The Auditor's Position on Status is based on inspection of evidence received during fieldwork. A follow-up on the open recommendations recorded in this report will occur during the next audit cycle or via the NRC OIG's status of recommendations process.

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
OIG-22-A-14 FY 2022 FISMA Audit	*FY 2022 Recommendation 1*: Review and update the Information Technology Infrastructure System (ITI) Core Services System Security Plan (SSP) System Interconnections tab and related security control implementation to ensure system interconnection details reflect the current system environment.	This recommendation is resolved. The NRC has converted the ITI SSP from NIST SP 800-53, Revision 4 to Revision 5. The NRC will ensure that related security control implementation details reflect the current system environment. Estimated target completion date: FY 2023 Quarter 2.	Open The ITI Core Services SSP security control implementation details for CA-3 System Interconnections notes that ITI has multiple connections with other systems in which the connection agreements are either expired or have not yet been created. Also, the ITI POA&M detail report indicates related POA&M ITI-17-2397 is open.
OIG-22-A-14 FY 2022 FISMA Audit	*FY 2022 Recommendation 2*: Implement a process to verify that remaining external interconnections noted in the ITI Core	This recommendation is resolved.	Open Same comments as

[26] See footnotes 22 and 23.

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
	Services SSP have documented, up-to-date Interconnection Security Agreement (ISA) / Memorandums of Understanding (MOUs) or Service Level Agreements (SLAs) in place as applicable.	The NRC's annual Periodic Security Control Assessment (PSCA) process includes a review of the external interconnections, ISA/MOUs, and SLAs within the ITI Core Services SSP Interconnection tab. The NRC will analyze its PSCA process and implement improvements to ensure that external interconnections noted in the ITI Core Services SSP are verified to be current and accurate. Estimated target completion date: FY 2023 Quarter 3.	above.
OIG-22-A-14 FY 2022 FISMA Audit	*FY 2022 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.	This recommendation is resolved. The NRC will ensure that the ITI inventory detail is updated and will correct any discrepancies and incorrect information identified for ITI assets in the Common Computing Services, Peripherals, Unified Communications, and Voice over Internet Protocol subsystem inventories. Estimated target completion date: FY 2023 Quarter 4.	Open The ITI Core Services SSP security control implementation details for CM-8 System Component Inventory notes an implementation status of planned and states: "During various PSCA efforts, it was revealed that the ITI inventory has multiple discrepancies and incorrect information listed for ITI devices." Also, the ITI POA&M

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
			detail report indicates related POA&M ITI-17-2401 is open.
OIG-22-A-14 FY 2022 FISMA Audit	*FY 2022 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 is resolved. The NRC will update the ITI PSCA process to include a verification that the associated IT asset inventory is current, complete, and accurate. All inventory inaccuracies will be documented, along with a recommended plan of action. Estimated target completion date: FY 2023 Quarter 4.	Open Same comments as above.
OIG-22-A-14 FY 2022 FISMA Audit	*FY 2022 Recommendation 5*: Implement a process to document the supply chain risk management requirements within the NRC information systems' system security plans.	This recommendation remains open. Estimated target completion date: FY 2024 Quarter 1.	Open For one (1) of three (3) systems selected for testing, Supply Chain Risk Management (SR) controls were not documented. Specifically, Business Applications Support System (BASS) was not incorporating NIST 800-53, Revision 5 controls for five (5) of its subsystems.
OIG-22-A-14 FY 2022 FISMA	*FY 2022 Recommendation 6*: Implement a process to validate that all personnel with	This recommendation is resolved.	Open

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
Audit	privileged level responsibilities complete annual security awareness and role-based training.	The NRC maintains an authoritative list of users with privileged level responsibilities as well as a database of associated role-based training. The Office of the Chief Information Officer (OCIO) and the Office of the Chief Human Capital Officer employ a collaborative process to ensure that all role-based training is completed by the annual target date of September 1. The process includes Training Management System reporting and continuous outreach to individual users and their respective supervisors and contracting officer's representatives. The NRC recently strengthened the accuracy of its authoritative list of users with privileged level responsibilities by implementing a weekly update process to capture new users as well as a redundant monthly update process to ensure completeness. As a result of this process, in FY 2022, 94 percent of users completed the training by the target date of September 1 and 98 percent completed the training by September 30. The NRC will analyze this process to identify and implement any further	For a sample of four (4) privileged network users from the population of 41 privileged network users with whenCreated dates since October 1, 2022, we noted that three (3) privileged network users did not complete required role-based training course assignments within one year of testing; and one (1) privileged network user did not complete their initial role-based training within one week of gaining access to their privileged account.

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		improvements that will increase its effectiveness. Estimated target completion date: FY 2023 Quarter 3.	
OIG-22-A-14 FY 2022 FISMA Audit	*FY 2022 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 is resolved. Providing security awareness training, which contains sensitive information, to new contractors outside the NRC's secure network would require the creation and ongoing maintenance of a separate secure system. The NRC does not believe that the benefit of new contractors completing the training before gaining access to the NRC network outweighs the costs of a separate secure system. Instead, 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 contractors gain access to the NRC network. In addition, the NRC will strengthen its process after onboarding to ensure that new contractors complete all required security awareness training, including acknowledging the Rules of Behavior, within the required 30-day timeframe.	Open For a sample 11 new network users from the population of 121 enabled network user accounts created since October 1, 2022 (employees and contractors), we noted that two (2) new users did not complete their initial security training requirements and acknowledgement of rules of behavior prior to accessing the NRC environment. The identified users were contractors.

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		Estimated target completion date: FY 2023 Quarter 3.	
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 1*: Reconcile mission priorities and cybersecurity requirements into profiles to inform the prioritization and tailoring of controls (e.g., High Value Assets (HVA) control overlays) to support the risk-based allocation of resources to protect the NRC's identified Agency level and/or National level HVAs.	This recommendation is resolved. The NRC will reconcile mission priorities and cybersecurity requirements to derive profiles to inform the prioritization and tailoring of controls to support the risk-based allocation of resources to protect the agency's identified agency- and national-level HVAs. Estimated target completion date: FY 2023 Quarter 2.	Open Evidence to support closure was not provided during fieldwork.
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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.	This recommendation remains open. In order to continue to aggregate security risks, normalize cybersecurity risk information across organizational units, and prioritize operational risk responses, the NRC is implementing a centralized and automated application that will aggregate cybersecurity POA&M risks for all FISMA systems, including the agency's programmatic cybersecurity POA&Ms. The application will also	Open

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		prioritize cybersecurity POA&M risks across organizational units. Estimated target completion date: FY 2024 Quarter 1.	
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 3*: Update procedures to include assessing the impacts to the organization's Information Security Architecture prior to introducing new information systems or major system changes into the Agency's environment.	This recommendation remains open. The NRC plans to propose the resources necessary to support this recommendation during formulation of the FY 2025 budget. The first full annual review is expected to occur in the fourth quarter (Q4) of FY 2025. Estimated target completion date: FY 2025.	Open
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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.	This recommendation remains open. The NRC is assessing strategies to modify its POA&M and business processes to include mechanisms for prioritizing completion and incorporating this as part of documenting a justification and approval for delayed POA&Ms. Estimated target completion date: FY 2024 Quarter 1.	Open
OIG-22-A-04 FY 2021 FISMA	*FY 2021 Recommendation 5*: Assess the NRC supply chain risk and fully define	The NRC recommends closure of this item.	Closed

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
Evaluation	performance metrics in service level agreements and procedures to measure, report on, and monitor the risks related to contractor systems and services.		The OIG reviewed a finalized and two in-draft procedures that the Supplemental Supply Chain Risk Assessment (SCRA) process provides a basis for measuring and monitoring metrics to assess risks associated with contractor systems and services. Therefore, this recommendation is considered closed.
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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 is resolved. The NRC has developed two draft computer security processes in CSO-PROS-0008 "Process to Assess, Respond, and Monitor ICT Supply Chain Risks" and CSO-PROS-0007" Process to Use SCR Investigation Service to Determine Information and Communications Technology (ICT) Supply Chain Risk Associated with an Offeror," issued August 8, 2022, that are currently being utilized to determine the supply chain risk associated with an ICT product or service and perform appropriate responsive actions and monitor the	Open Evidence to support closure was not provided during fieldwork.

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		risk over time. NRC will finalize the processes once a sufficient number of assessments are performed to determine the effectiveness of the evaluations. Estimated target completion date: FY 2023 Quarter 3.	
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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. The NRC is assessing approaches to implement the processes for the 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. Estimated target completion date: FY 2023 Quarter 4.	Open
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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. Pursuant to the Supply Chain Security Training Act of 2021, Pub. L. 117-145, General Services Administration (GSA) is required to develop training for federal officials with supply chain risk management	Open Evidence to support closure was not provided during fieldwork.

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		responsibilities. The NRC will leverage this training, which will be implemented by Office of Management and Budget (OMB), when it becomes available. Estimated target completion date: FY 2023 Quarter 1.	
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 10*: Centralize system privileged and non-privileged user access review, audit log activity monitoring, and management of Personal Identity Verification (PIV) or Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential access to all NRC systems (findings noted in bullets a, and c, above) by continuing efforts to implement these capabilities using the Splunk QAudit, SailPoint, and CyberArk automated tools.	The NRC recommends closure of this item.	Closed The OIG met with OCIO to view the centralized system privileged and non-privileged user access review, audit log activity monitoring, and management of PIV or IAL 3 / AAL 3 credential access to all NRC systems. Therefore, this recommendation is considered closed.
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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.	The NRC recommends closure of this item. The NRC implemented an updated procedure that requires users to complete nondisclosure and rules of behavior agreements as part of the onboarding process prior to being granted access to NRC	Open The NRC should update user system access control procedures to include the requirement for individuals to complete a non-disclosure and

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		systems and information. The NRC Office of Administration began using the new process, which is part of Personal Identity Verification (PIV) card enrollment, on December 9, 2020.	rules of behavior agreements prior to the individual being granted access to NRC systems and information. Specifically, for a sample 11 new network users from the population of 121 enabled network user accounts created since October 1, 2022 (employees and contractors), we noted that two (2) new users did not complete their initial security training requirements and acknowledgement of rules of behavior prior to accessing the NRC environment. The identified users were contractors.
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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.	This recommendation remains open. The NRC will conduct an in-depth, independent assessment of the agency's privacy program. Using the results of the assessment, the	Open The NRC has not yet completed an independent review or assessment of the NRC privacy program and used the results of

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		NRC will periodically update the privacy program. Estimated target completion date: FY 2024 Quarter 1.	these reviews to periodically update the privacy program. The NRC has engaged a contractor to perform an independent assessment of the NRC's Privacy Program. However, the assessment was ongoing at the time of our review.
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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 is resolved. The NRC will perform an analysis to determine the best and most economical path forward to administer computer security training to new NRC employees and contractors before they gain access to the agency's systems. Estimated target completion date: FY 2023 Quarter 3.	Open For a sample 11 new network users from the population of 121 enabled network user accounts created since October 1, 2022 (employees and contractors), we noted that two (2) new users did not complete their initial security training requirements and acknowledgement of rules of behavior prior to accessing the NRC environment. The identified users were contractors.

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
			For a sample of four (4) privileged network users from the population of 41 privileged network users with whenCreated dates since October 1, 2022, we noted that three (3) privileged network users did not complete required role-based training course assignments within one year of testing; and one (1) privileged network user did not complete their initial role-based training within one week of gaining access to their privileged account.
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 14*: 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 is resolved. The NRC has implemented the technical capability to restrict NRC network access for employees who do not complete annual security awareness training. To date, this capability has been deployed to restrict NRC network access for contract personnel who do not complete annual security	Open Same comments as above.

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		awareness training on time. Deploying this capability for NRC employees, however, would require alignment with several agency stakeholders. The NRC closely tracks the timely completion of training by its employees resulting in the majority of employees completing the training on time. In light of these factors, the NRC is continuing to assess the need to deploy this capability for employees. Estimated target completion date: FY 2023 Quarter 3.	
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 15*: Implement metrics to measure and reduce the time it takes to investigate an event and declare it as a reportable or non-reportable incident to United States Computer Emergency Readiness Team (US-CERT).	The NRC recommends closure of this item.	Closed The OIG reviewed the updated standard operating procedure and an incident reporting form that is used to input information into the database for tracking and metric measurement. Therefore, this recommendation is considered closed.
OIG-22-A-04 FY 2021 FISMA	*FY 2021 Recommendation 16*: Conduct an organizational level Business Impact Analysis	This recommendation remains open.	Open

U.S. Nuclear Regulatory Commission
FY 2023 Audit of the NRC's Implementation of the FISMA

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
Evaluation	(BIA) to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.	The NRC will conduct an organization-level BIA to determine contingency planning requirements and priorities, including for mission essential functions and HVAs, and update contingency planning policies and procedures accordingly. Due to limited resources and other priority operational and cybersecurity work, the NRC is now targeting completion in FY 2024. Estimated target completion date: FY 2024 Quarter 3.	
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 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. The NRC will 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. Due to limited resources and other priority	Open

Report No.	Recommendation	NRC's Status	Auditor's Position on Status
		operational and cybersecurity work, the NRC is now targeting completion for FY 2024. Estimated target completion date: FY 2024 Quarter 4.	
OIG-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 18*: Update and implement procedures to coordinate contingency plan testing with ICT supply chain providers.	This recommendation remains open. The NRC is assessing approaches to implement procedures to coordinate contingency plan testing with ICT supply chain providers. Due to limited resources and other priority operational and cybersecurity work, the NRC is now targeting completion in FY 2024. Estimated target completion date: FY 2024 Quarter 4.	Open

NRC's MANAGEMENT COMMENTS

An exit briefing was held with the agency on August 30, 2023. Prior to this meeting, 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.