MEMORANDUM

DATE: September 29, 2022

TO: Daniel H. Dorman
Executive Director for Operations

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

SUBJECT: AUDIT OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2022 (OIG-22-A-14)

The Office of the Inspector General (OIG) contracted with CliftonLarsonAllen LLP (CLA) to conduct an audit of the United States Nuclear Regulatory Commission's (NRC) Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2022. Attached is CLA's report *Audit of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2022*. 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, agency staff indicated that they had no formal comments for inclusion in this report.

For the period October 1, 2021, through July 30, 2022, 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

Audit of the United States Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014

Fiscal Year 2022

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
CLAconnect.com

September 28, 2022

Robert J. Feitel
Inspector General
United States Nuclear Regulatory Commission
Office of the Inspector General
11555 Rockville Pike
Rockville, MD 20852

Dear Mr. Feitel:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the results of our audit of the U.S. Nuclear Regulatory Commission's (NRC or Agency) information security program and practices for fiscal year 2022 in accordance with the Federal Information Security Modernization Act of 2014.

We appreciate the assistance we received from the NRC. We will be pleased to discuss any questions you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
United States Nuclear Regulatory Commission

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the U.S. Nuclear Regulatory Commission's (NRC or Agency) information security program and practices for fiscal year (FY) 2022 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an agency-wide information security program. In addition, FISMA requires Inspectors General 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

For this year's review, Inspectors General were required to assess 20 Core Inspector General (IG) FISMA Reporting Metrics in 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, an agency's information security program must be rated Level 4 – *Managed and Measurable*.

The audit included an assessment of the NRC's information security program and practices consistent with 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, Maryland from April to July 2022. The audit covered the period from October 1, 2021, through July 30, 2022.

We concluded that the NRC implemented effective information security policies, procedures, and practices by achieving an overall Level 4 - *Managed and Measurable* maturity level for an effective information security program. Although the NRC implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted weaknesses in the risk management, supply chain risk management, identity and access management, security training, and information security continuous monitoring domains of the FY 2022 IG FISMA Reporting Metrics. As a result, we made seven new recommendations to assist the NRC in strengthening its information security program. Additionally, we noted 13 prior year recommendations remain open.

[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 28, 2022. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 28, 2022.

The purpose of this audit report is to report on our assessment of the NRC's compliance with 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 28, 2022

Table of Contents

EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also requires agency Inspectors General 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 fiscal year (FY) 2022 Core Inspector General (IG) FISMA Reporting Metrics requires us to assess the maturity of five functional areas in the NRC's information security program and practices. For this year's review, Inspectors General were required to assess 20 Core Metrics in 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.[2] 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 FY 2022 Core IG FISMA Reporting Metrics and FISMA reporting requirements.

The audit included an assessment of the NRC's information security programs and practices consistent with FISMA and reporting instructions issued by the OMB. In addition, we reviewed selected controls mapped to the FY 2022 Core IG FISMA Reporting Metrics for a sample of three of 17 information systems[3] in the NRC's FISMA inventory of information systems as of April 2022.[4]

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[2] The function areas are further broken down into nine domains.
[3] 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.
[4] NRC's FISMA inventory of information systems details a list of NRC's FISMA reportable systems.

Audit Results

We concluded that the NRC implemented effective information security policies, procedures, and practices by achieving an overall Level 4 - *Managed and Measurable* maturity level for an effective information security program. For example, the NRC:

- Conducted periodic security control assessments.
- Maintained an effective incident response program.
- Maintained an effective continuous monitoring program including dashboards for tracking risk management posture.

Table 1 below shows a summary of the overall assessed maturity levels for each function area and domain in the FY 2022 Core IG FISMA Reporting Metrics.

Table 1: Assessed Maturity Levels for FY 2022 Core 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 2: Defined
Protect	Level 4: Managed and Measurable	**Configuration Management**	Level 4: Managed and Measurable
		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 weaknesses in the risk management, supply chain risk management, identity and access management, security training, and information security continuous monitoring domains of the FY 2022 IG FISMA Reporting Metrics (see **Table 2**). As a result,

we made seven new recommendations to assist the NRC in strengthening its information security program. Additionally, we noted 13 prior year recommendations remain open.[5]

Table 2: Weaknesses Noted in FY 2022 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2022 Core IG FISMA Reporting Metrics

Cybersecurity Framework Security Function	FY 2022 Core IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	Weakness with Documenting Interconnections Accurately (**Finding 1**) Weaknesses in the Accuracy of System Component Inventory (**Finding 2**)
	Supply Chain Risk Management	Weaknesses in System Level Implementation of Supply Chain Risk Management Controls (**Finding 3**)
Protect	**Configuration Management**	No weaknesses noted.
	Identity and Access Management	Weaknesses in Completion of Training Requirements for Privileged Users and New Users (**Finding 4**)
	Data Protection and Privacy	No weaknesses noted.
	Security Training	Weaknesses in Completion of Training Requirements for Privileged Users and New Users (**Finding 4**)
Detect	**Information Security Continuous Monitoring**	Weakness with Documenting Interconnections Accurately (**Finding 1**)
Respond	**Incident Response**	No weaknesses noted.
Recover	**Contingency Planning**	No weaknesses noted.

The following section provides a detailed discussion of the audit findings. **Appendix I** provides background information on FISMA. **Appendix II** describes the audit objective, scope, and methodology. **Appendix III** provides the status of prior year recommendations. **Appendix IV** includes the NRC's management comments.

[5] See Appendix III for detailed status of prior year recommendations.

AUDIT FINDINGS

1. Weakness with Documenting Interconnections Accurately

Cybersecurity Framework Security Function: *Identify and Detect*
FY 2022 Core IG FISMA Reporting Metrics Domain: *Risk Management and Information Security Continuous Monitoring*

The Information Technology Infrastructure System (ITI) Core Services System Security Plan (SSP) contains inaccurate information related to interconnections. Specifically, the ITI Core Services SSP System Interconnections tab includes details of connections to either internal systems, subsystems, a decommissioned system, a system transitioned to another authorization boundary or commercial entities covered by service level agreements (SLAs). The ITI Core Services SSP System Interconnections tab also indicates that interconnection security agreements (ISAs) and memoranda of understanding (MOUs) for external system interconnections to ITI are either expired based on the date of agreement or have not yet been created and the date is to be determined.

The System Interconnections tab and related interface controls were not a focal point of annual review and update of the ITI Core Services SSP. In addition, the System Interconnections tab was used as a repository for details of internal connections and external interconnections (i.e., interfaces). NRC management is in the process of confirming the details of the systems and is revising the System Interconnections tab and related interface controls to reflect the current operating environment.

NIST Special Publication SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, security controls state, in part:

> PL-2: System Security and Privacy Plans
> Control:
> …
> c. Review the plans [*Assignment: organization-defined frequency*];
> d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments;
>
> CA-3: Information Exchange
> Control:
> a. Approve and manage the exchange of information between the system and other systems using [*Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement*]];
> b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
> c. Review and update the agreements [*Assignment: organization-defined frequency*].

CA-9: Internal System Connections
Control:
…
b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
c. Terminate internal system connections after [*Assignment: organization-defined conditions*]; and
d. Review [*Assignment: organization-defined frequency*] the continued need for each internal connection.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. Therefore, if current details on information exchange and system connections are not maintained in the system security plan, any risk treatment decisions made by authorizing officials regarding them may be based on incomplete or inaccurate information.

We recommend that NRC management:

Recommendation 1: *Review and update the ITI Core Services SSP System Interconnections tab and related security control implementation to ensure system interconnection details reflect the current system environment.*

Recommendation 2: *Implement a process to verify that remaining external interconnections noted in the ITI Core Services SSP have documented, up-to-date ISA/MOUs or SLAs in place as applicable.*

2. Weaknesses in the Accuracy of System Component Inventory

Cybersecurity Framework Security Function: *Identify*
FY 2022 Core IG FISMA Reporting Metrics Domain: *Risk Management*

The ITI subsystems' component inventories have multiple discrepancies and incorrect information listed for ITI devices tracked in four of 12 subsystem component inventories.

At the time of our review, there were related open plans of action and milestones (POA&Ms). These POA&Ms indicated that inventory details did not consistently include all the NRC required information. Some examples of missing information from ITI subsystem inventories include: Asset Role, Asset Type, Virtual or Physical Device, Virtual Machine/Instance Host (server or cluster), Manufacturer, Manufacturer Model Number/Version, Manufacturer Serial Number, Operating System Name, Operating System Version and Licensing Information.

NIST SP 800-53 Revision 5, Configuration Management (CM) security control CM-8, System Component Inventory, states:

Control:
a. Develop and document an inventory of systems components that:
    1. Accurately reflects the system;

2. Includes all components within the system;
3. Does not include duplicate accounting of components or components assigned to any other system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability: [*Assignment: organization-defined information deemed necessary to achieve effective system component accountability*]; and

b. Review and update the system component inventory [*Assignment: organization-defined frequency*].

In addition, within the *ITI Core Services SSP*, dated February 2022, the organizationally defined values for security control CM-8 states:

> The organization develops and documents an inventory of information system components that includes:
> - System Name
> - Asset Role (e.g., Windows Domain Controller vs. Windows Member Server; Perimeter Switch vs. Infrastructure Switch)
> - Asset Type (e.g., firewall, server, workstation)
> - Virtual or Physical Device
> - Virtual Machine/Instance Host (server or cluster)
> - Manufacturer
> - Manufacturer Model Number/Version
> - Manufacturer Serial Number
> - Asset Tag (if owned/leased by the NRC)
> - Unique Host Name (if available, the host's fully qualified domain name)
> - Location (i.e., site, building, and room where the asset is located)
> - Operating System Name
> - Operating System Version
> - Licensing Information
> - License Expiration Date
>
> The organization reviews and updates the information system component inventory at least annually and within 30 days of hardware or software changes within the system.

Inaccurate subsystem inventory information can compromise component accountability for ITI. In addition, inaccurate subsystem inventory information can impact the integrity of decisions made about ITI asset life cycle management, tracking and reporting.

We recommend that NRC management:

> ***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.*
>
> ***Recommendation 4:*** *Document and implement a periodic review of subsystem inventories to verify information maintained for each ITI subsystem is current, complete, and accurate.*

3. Weaknesses in System Level Implementation of Supply Chain Risk Management Controls

Cybersecurity Framework Security Function: *Identify*
FY 2022 Core IG FISMA Reporting Metrics Domain: *Supply Chain Risk Management*

The supply chain risk management controls encompassed within the scope of NIST SP 800-53 Revision 5, were not within SSPs for three of three sampled systems (ITI, Safeguards Information Local Area Network and Electronic Safe [SLES], and Operations Center Information Management System [OCIMS]).

The NRC is in the process of transitioning to NIST SP 800-53, Revision 5, as the supplementary assessment guidance was not released until January 2022. In addition, the NRC plans to fully implement NIST SP 800-53, Revision 5, by January 2023 and will have incorporated the associated supply chain risk management controls into the respective system security plans by that time.

NIST SP 800-53, Revision 5, supply chain risk management (SR) security control SR-3 Supply Chain Controls and Processes, states the following:

> Control:
> a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [*Assignment: organization-defined system or system component*] in coordination with [*Assignment: organization-defined supply chain personnel*];
> b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: [*Assignment: organization-defined supply chain controls*]; and
> c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [*Assignment: organization-defined document*]].

Without fully addressing supply chain risk management processes in the NRC's procedures, certain supply chain risk management processes may not be fully implemented. This may hinder the NRC's ability to identify and mitigate supply chain risks at the system level.

We recommend that NRC management:

> ***Recommendation 5:*** *Implement a process to document the supply chain risk management requirements within the NRC information systems' system security plans.*

4. Weaknesses in Completion of Training Requirements for Privileged Users and New Users

Cybersecurity Framework Security Function: *Protect*
FY 2022 Core IG FISMA Reporting Metrics Domain: *Identity and Access Management and Security Training*

We noted the following weaknesses related to training requirements for privileged users and new users:

- For a sample of six privileged ITI users from the population of 64 new privileged ITI users, one privileged ITI user did not complete mandatory annual security awareness and role-based training and three privileged ITI users did not complete annual role-based training.

  Upon notification of the issue, management indicated that three individuals had subsequently completed the required role-based training and the remaining individual had until September 1, 2022, to complete the outstanding security awareness and role-based training or they would face access disablement.

- We were unable to validate that initial security training requirements and signed Rules of Behavior were completed for four contractors out of a sample of 25 new employees and contractors from the total population of 93 new employees and 189 new contractors.

NRC management indicated that the process for tracking role-based training and monitoring completion of initial security training requirements and rules of behavior was a manual process. Additionally, NRC management indicated that there is limited visibility into the Contracting Officer's Representative (COR) oversight of its contractors to ensure completion of training and rules of behavior.

The *Nuclear Regulatory Commission Common Controls (NRCcc) Information Security Program Plan*, dated July 27, 2021, implementation details and organizationally defined values for the following security controls state, in part:

> AT-2: Security Awareness Training
> Control:
> a. The Office of the Chief Human Capital Officer (OCHCO) provides agency-wide cybersecurity awareness training courses, developed with input by the Computer Security Officer (CSO), via the NRC Talent Management System (TMS) to all NRC system users (including managers, senior executives, and contractors) for new users and annually thereafter. Office Directors, Regional Administrators, and Technical Training Center (TTC) ensure that all staff and contractors for whom they are responsible and who have access to NRC electronic information are identified within the NRC learning system (TMS), have the required accounts within TMS, and ensure the completion of required cybersecurity awareness training.

AT-3: Role-Based Security Training
Control:

a. OCHCO, with input from CSO, provides agency-specific role-based cybersecurity training for personnel with security roles defined in the Cybersecurity Role-Requirements Matrix located on the CSO Training and Awareness site.
b. NRC users are required to take role-based training before the users are authorized to access information systems and/or perform assigned duties, or when system changes occur.

PL-4: Rules of Behavior
Control:

…

b. The CSO requires electronic acknowledgment of Agency-wide Rules of Behavior from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and NRC systems and annually thereafter via annual security awareness training.

Without providing annual role-based training to individuals with elevated privileges and responsibilities, those personnel are not receiving more detailed training about processes for handling their position and ensuring a secure environment. In addition, the NRC may be at an increased risk of individuals misusing their roles if not properly trained for their position.

Furthermore, without providing adequate security awareness training and rules of behavior to individuals, those personnel may not receive proper awareness of risk and procedures for ensuring a secure environment. The NRC may also be at an increased risk of new contractors or new employees obtaining access to systems without having read, understood, and agreed 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 that NRC management:

Recommendation 6: *Implement a process to validate that all personnel with privileged level responsibilities complete annual security awareness and role-based training.*

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.*

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 Chairman. 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)

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. 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. FISMA requires agency heads to take the following actions, among others:[6]

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.

[6] 44 USC § 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, FISMA requires agency Inspectors General to assess the effectiveness of their agency's information security program and practices.

National Institute of Standards and Technology (NIST) Security Standards and Guidelines

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. 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 Department of Homeland Security (DHS) annually provide instructions to Federal agencies and Inspectors General for preparing FISMA reports. On December 6, 2021, the OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*. 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 and highly valuable controls that Inspectors General must evaluate annually. The Core Metrics can be found in the *OMB Office of the Federal Chief Information Officer FY 2022 Core IG Metrics Implementation Analysis and Guidelines*. The remainder of standards and controls will be evaluated on a two-year cycle.
- The OMB also shifted the due date of the IG FISMA Reporting Metrics from October to July to better align with the release of the President's Budget. Use of this reporting timeline began in FY 2022 starting with the Core Metrics.

The FY 2022 Core IG FISMA Reporting Metrics provided the reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.

For this year's review, Inspectors General were to assess 20 Core IG FISMA Reporting Metrics in 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 Core 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**.

U.S. Nuclear Regulatory Commission
FY 2022 Audit of NRC's Implementation of the FISMA

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2022 Core IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Domains in the FY 2022 Core 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 Core 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

For this year's review, Inspectors General were to assess 20 Core IG FISMA Reporting Metrics in 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 scope of this performance audit was to assess the NRC's information security program and practices consistent with FISMA and reporting instructions issued by the OMB and the DHS. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, mapped to the FY 2022 Core IG FISMA Reporting Metrics, for a sample of three of 17 information systems in the NRC's FISMA inventory of information systems as of April 2022 **(Table 5)**.

Table 5: Description of Systems 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.
Safeguards Information Local Area Network and Electronic Safe (SLES)	The SLES system stores and manages electronic SGI documentation. SLES contains two distinct components: a secure Local Area Network (LAN) and an electronic safe (E-Safe) for SGI documents.

System Name	Description
Operations Center Information Management System (OCIMS)	OCIMS supports the NRC Operations Center during daily activities, regularly scheduled exercises, and reported emergencies by providing common access to data for the staff located at the NRC Headquarters Operations center (HOC) and the NRC Regional Incident Response Centers (IRC). OCIMS is the primary means of creating, storing, sending and retrieving information in the NRC Operations Center and is referred to as the OCIMS LAN. OCIMS is an integrated system comprised of three subsystems: Data, Display and Voice Subsystems.

The audit also included an evaluation of whether the NRC took corrective action to address open recommendations from the FY 2021 FISMA evaluation.[7]

Audit fieldwork covered the NRC's headquarters located in Rockville, Maryland from April to July 2022. The audit covered the period from October 1, 2021, through July 30, 2022.

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 FISMA. Also, we reviewed documents supporting the information security program. These documents included, but were not limited to, 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 audit recommendations.[8] 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:

- OMB Memorandum M-22-05 *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.
- OMB Office of the Federal Chief Information Officer *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*.
- Council of the Inspectors General on Integrity and Efficiency (CIGIE), the OMB, the DHS, and the Federal Chief Information Officers and Chief Information Security Officers councils *FY 2022 Core IG FISMA Metrics Evaluation Guide.*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* for specification of security controls.

[7] *Independent Evaluation Report of the NRC's Implementation of FISMA 2014 For Fiscal Year 2021* (Report No. OIG-22-A-04, issued December 20, 2021).
[8] Ibid. footnote 7.

- 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 800-53B, *Control Baselines for Information Systems and Organizations.*
- 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.
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).
- NRC policies and procedures, including but not limited to:
  - *ITI Core Services System Security Plan*
  - *NRCcc Information Security Program Plan*

We selected three NRC information systems from the total population of 17 FISMA reportable systems for testing. The three systems were selected based on risk, date of last evaluation, High Value Asset (HVA) status and criticality. Specifically, the ITI system was selected based on risk since it is categorized as a moderate impact system[9] and supports the NRC's applications that reside on the network. The SLES application was selected because it is categorized as a high impact system, is considered a HVA and was last evaluated in 2013. The third system selected for testing was OCIMS, a moderate impact system that was last evaluated in 2015. We tested the three systems' selected security controls to support our responses to the FY 2022 Core 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.

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

U.S. Nuclear Regulatory Commission
FY 2022 Audit of NRC's Implementation of the FISMA

STATUS OF PRIOR RECOMMENDATIONS

The table below summarize the status of the prior year recommendations from the FY 2021 FISMA evaluation.[10]

Recommendation Number	Recommendation	NRC's Status	Auditor's Position on Status
1	Reconcile mission priorities and cybersecurity requirements into profiles to inform the prioritization and tailoring of controls (e.g., HVA control overlays) to support the risk-based allocation of resources to protect the U.S. NRC's identified Agency level and/or National level HVAs.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 2.	Open
2	Continue current Agency's efforts to update the Agency's cybersecurity risk register to (i) aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.	This recommendation is closed. We noted that the NRC has implemented supporting reviews done through their Federal Information Technology Acquisition Reform Act (FITARA) process and dashboards that aggregate security risks.	Closed
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. Estimated target completion date: FY 2023 Quarter 1	Open
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 is closed. The NRC POA&M process has been revised to incorporate clarified requirements for prioritization on the basis of POA&M status and weakness severity / classification.	Closed

[10] Ibid. footnote 7.

U.S. Nuclear Regulatory Commission
FY 2022 Audit of NRC's Implementation of the FISMA

Recommendation Number	Recommendation	NRC's Status	Auditor's Position on Status
5	Assess the NRC supply chain risk and fully define performance metrics in service level agreements and procedures to measure, report on, and monitor the risks related to contractor systems and services.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 3.	Open
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 closed. The NRC policies and procedures have been documented and implemented to encompass a risk-based process for evaluating cyber supply chain risks associated with third party providers.	Closed
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 2023 Quarter 4.	Open
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 2023 Quarter 1.	Open
9	Continue to monitor the remediation of critical and high vulnerabilities and identify a means to assign and track progress of timely remediation of vulnerabilities.	This recommendation is closed.	Closed
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 Security Information and Event Management, Audit	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 1.	Open

U.S. Nuclear Regulatory Commission
FY 2022 Audit of NRC's Implementation of the FISMA

Recommendation Number	Recommendation	NRC's Status	Auditor's Position on Status
	Analytics, and Identity Security and Access Management Solutions automated tools.		
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 2022 Quarter 4.	Open
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. Estimated target completion date: FY 2022 Quarter 3.	Open
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 2023 Quarter 1.	Open
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 remains open. Estimated target completion date: FY 2023 Quarter 1.	Open
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 the United States Computer Emergency Readiness Team (US-CERT).	This recommendation is closed. The *NRC Computer Security Incident Response Team (CSIRT) Standard Operating Procedures* features metrics related to incident response. There are also various metrics tracked through dashboards and Situational Awareness Reports.	Closed

U.S. Nuclear Regulatory Commission
FY 2022 Audit of NRC's Implementation of the FISMA

Recommendation Number	Recommendation	NRC's Status	Auditor's Position on Status
16	Conduct an organizational level Business Impact Analysis (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 2023 Quarter 3.	Open
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 2023 Quarter 4.	Open
18	Update and implement procedures to coordinate contingency plan testing with Information, Communication and Technology (ICT) supply chain providers.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 4.	Open

APPENDIX IV: NRC's MANAGEMENT COMMENTS

An exit briefing was held with the agency on September 21, 2022. 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.