MEMORANDUM

DATE: September 29, 2023

TO: Katherine Herrera
Acting Executive Director of Operations

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

SUBJECT: AUDIT OF THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023 (DNFSB-23-A-04)

The Office of the Inspector General (OIG) contracted with CliftonLarsonAllen LLP (CLA) to conduct the *Audit of the Defense Nuclear Facilities Safety Board's (DNFSB) 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 DNFSB. 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 formal comments for inclusion in this report.

For the period October 1, 2022, through June 30, 2023, CLA found that the DNFSB did not establish an effective agency-wide information security program, and there were weaknesses that impact the agency's ability to adequately protect the DNFSB's system 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: T. Tadlock, OEDO

Audit of the Defense Nuclear Facilities Safety Board'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
Defense Nuclear Facilities Safety Board

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Defense Nuclear Facilities Safety Board's (DNFSB) information security program and practices for fiscal year (FY) 2023 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an agency-wide information security program. In addition, 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 DNFSB.

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, DNFSB's information security program must be rated Level 4 – *Managed and Measurable*.

The audit included an assessment of the DNFSB's information security programs 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 the DNFSB General Support System (GSS).

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

We concluded that the DNFSB did not implement effective information security policies, procedures and practices, since it achieved an overall *Level 3 – Consistently Implemented* maturity level. A *Level 3* designation reflects that although an agency's policies, procedures, and strategy are consistently implemented, quantitative and qualitative effectiveness measures are lacking. Therefore, the DNFSB did not have an effective information security program.

We noted new and repeat weaknesses in seven of the eight domains of the FY 2023 IG FISMA Reporting Metrics. As a result, we made 1 new recommendation to assist the DNFSB in strengthening its information security program. Additionally, 35 prior year recommendations remain open dating back to FY 2019.

[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 DNFSB on or before September 15, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 15, 2023.

The purpose of this audit report is to report on our assessment of the DNFSB'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 15, 2023

Table of Contents

EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also requires agency Inspector Generals (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 Nuclear Regulatory Commission and Defense Nuclear Facilities Safety Board (DNFSB) 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 DNFSB'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 DNFSB.

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 DNFSB's information security program and practices consistent with FISMA and reporting instructions issued by the OMB. In addition, we reviewed selected controls from NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2023 IG FISMA Reporting Metrics for the DNFSB General Support System (GSS).
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,

[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 DNFSB 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.

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 DNFSB did not implement effective information security policies, procedures and practices, since it achieved an overall *Level 3 – Consistently Implemented* maturity level, and therefore the DNFSB did not have an effective information security program.[7] To be considered effective, DNFSB's information security program must be rated *Managed and Measurable (Level 4).* **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 2: Defined	**Risk Management**	Level 3: Consistently Implemented
		Supply Chain Risk Management	Level 1: Ad-Hoc
Protect	Level 3: Consistently Implemented	**Configuration Management**	Level 3: Consistently Implemented
		Identity and Access Management	Level 4: Managed and Measurable
		Data Protection and Privacy	Level 3: Consistently Implemented
		Security Training	Level 4: Managed and Measurable
Detect	Level 2: Defined	**Information Security Continuous Monitoring**	Level 2: Defined
Respond	Level 3: Consistently Implemented	**Incident Response**	Level 3: Consistently Implemented
Recover	Level 3: Consistently Implemented	**Contingency Planning**	Level 3: Consistently Implemented
Overall	**Level 3: Consistently Implemented – Not Effective**		

In evaluating the effectiveness of the DNFSB's information security program, we considered the following factors:

- The DNFSB's size, complexity, and control environment were taken into consideration in the aggregate to raise the overall assessed maturity level.
- The OMB considers the 20 Core Metrics to be the most critical to determine the effectiveness of an Agency's information security program. The 20 FY 2023 supplemental metrics represent

[7] 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.

additional important activities conducted by security programs. Taken together, these metrics support assessment of the adoption of current administration priorities and contribute to the overall determination of DNFSB's security program effectiveness.

- The DNFSB has a significant number of open prior year recommendations. Since last year, the agency demonstrated actions to close 21 of the 56 open prior FISMA recommendations since FY 2019. In addition, there were prior year recommendations with significant impact to the FY 2023 IG FISMA Reporting Metrics which remain outstanding. The number of remaining prior year recommendations signifies that DNFSB has not gained momentum in addressing the underlying root causes of these security weaknesses.

To fully progress towards "Managed and Measurable," the DNFSB will need to address new and repeat weaknesses in its security program related to the risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, information security continuous monitoring, 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 1 new recommendation to assist the DNFSB in strengthening its information security program. Additionally, we noted 35 prior year recommendations remain open.[8] **Table 2** also includes weaknesses where DNFSB has prior year recommendations that remain open related to the FY 2023 IG FISMA Reporting Metrics.

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**	Open prior year recommendations related to security assessment authorization process.[9]
	Supply Chain Risk Management	Open prior year recommendation related to the supply chain risk management strategy.
Protect	**Configuration Management**	Open prior year recommendations related to the vulnerability management program.
	Identity and Access Management	Open prior year recommendation related to completing access agreements prior to granting system access.
	Data Protection and Privacy	Open prior year recommendation related to role-based privacy training.
	Security Training	No weaknesses noted.
Detect	**Information Security Continuous Monitoring**	Open prior year recommendations related to security assessment and risk management processes.
Respond	**Incident Response**	Weaknesses in DNFSB's Event Logging Maturity **(Finding 1)**.

[8] See appendix III for status of prior year recommendations.
[9] See appendix III for status of prior year open recommendations.

Cybersecurity Framework Security Function	FY 2023 IG FISMA Reporting Metrics Domain	Weaknesses Noted
Recover	**Contingency Planning**	Prior year recommendations open related to business impact analysis and contingency planning role-based training.

In order to demonstrate measurable improvements towards an effective information security program, the DNFSB needs to focus attention on remediating prior year recommendations in a timely manner and prioritizing those recommendations that relate to the Core Metrics. Implementing more of these recommendations will help the DNFSB to mature its information security program and bring it closer to effectiveness. In addition, DNFSB could consider developing a strategy to include resource commitments to address corrective actions necessary to show steady, measurable improvement in the DNFSB's information security program. Developing such a strategy may require the DNFSB to allocate sufficient resources, including staffing, to be responsible for remediating audit recommendations in a timely manner.

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 DNFSB's management comments.

AUDIT FINDINGS

1. Weaknesses in DNFSB's Event Logging Maturity

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

DNFSB assessed their Event Logging (EL) maturity against the requirements in the 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, [10] not-effective.

While DNFSB is developing a plan to assist with reaching compliance with OMB M-21-31 requirements, DNFSB did not reach EL1[11] and EL2[12] maturity levels by OMB's required due dates. Specifically, DNFSB 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, DNFSB did not document any risk-based decisions, including compensating controls, for not meeting the requirements in OMB M-21-31.

DNFSB management indicated that due to resource issues they were unable 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*[13] (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 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 Security Information and Event Management (SIEM).[14]

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:

[10] 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.
[11] Per OMB M-21-31, EL1 maturity level signifies only logging requirements of highest criticality are met.
[12] Per OMB M-21-31, EL2 maturity level signifies logging requirements of highest and intermediate criticality are met.
[13] See Executive Order 14028 online here.
[14] 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.

- 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]
- 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)

The agency and all its components meet the following requirements, as detailed in 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, DNFSB is not meeting logging requirements of highest criticality. DNFSB maturity is currently at EL0 maturity; therefore, their event logging capabilities are not effective based on OMB M-21-31. Further, DNFSB 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 DNFSB may not collect all meaningful and relevant data on suspicious events. This may, in turn increase the risk that DNFSB may inadvertently miss the potential scope or veracity of suspicious events or attacks.

Recommendation 1: We recommend that DNFSB's Chief Information Security Officer acquire resources 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.

EVALUATION OF MANAGEMENT COMMENTS

In response to a draft of this report, DNFSB agreed with the OIG's assessment of the current state of its information security program. In addition, DNFSB recognized that 21 prior year recommendations were closed based on inspection of evidence received during fieldwork for the FY 2023 FISMA audit. DNFSB management stated that another 8 prior year recommendations were closed; however, evidence required to verify closure of these recommendations was not provided during fieldwork. A follow-up on the open recommendations recorded in this report will occur during the next audit cycle or via the OIG's status of recommendation process. DNFSB's comments are included in **Appendix IV.**

BACKGROUND

Overview

The DNFSB, an independent executive branch agency, is charged with providing technical safety oversight of the Department of Energy's (DOE) defense nuclear facilities and activities in order to provide adequate protection for the health and safety of the public and workers. DNFSB's primary mission is to promote the protection of public health and safety by ensuring implementation of safety standards at DOE defense nuclear facilities and operations. In addition to conducting safety oversight on hundreds of existing hazardous nuclear operations, the DNFSB is obligated by law to conduct in-depth reviews of new DOE defense nuclear facilities during both design and construction.

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:[15]

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.

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 IGs to assess the effectiveness of their agency's information security program and practices.

[15] 44 USC § 3554, Federal agency responsibilities.

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 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*.[16] This memorandum described key changes to the methodology for conducting FISMA audits, as well as the processes for Federal agencies to report to OMB, and where applicable, 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.[17] 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.

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**.

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

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 DNFSB.

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, 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[18] 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.
The scope of this performance audit was to assess the DNFSB's information security program

[18] 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.

and practices consistent with 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 the DNFSB GSS.

Table 5: Description of System Selected for Testing

System Name	Description
DNFSB GSS	The purpose of the system is to provide a common set of services (user authentication, file & print, backup, etc.) that support the mission of the agency as well as all applications operated by DNFSB. All of DNFSB's organizations (Office of the General Counsel (OGC), Office of the General Manager (OGM), Office of the Technical Director (OTD), on-site contractors, as well as DNFSB members themselves are users of the system.

The audit also included an evaluation of whether the DNFSB took corrective action to address open recommendations from the FY 2022 FISMA audit,[19] FY 2021 FISMA evaluation,[20] FY 2020 FISMA evaluation,[21] and FY 2019 FISMA evaluation.[22]

Audit fieldwork covered the DNFSB's headquarters located in Washington, D.C. from January 2023 to June 2023. The audit covered the period from October 1, 2022, through June 30, 2023.

Methodology

To determine if the DNFSB implemented an effective information security program, we conducted interviews with DNFSB 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, DNFSB'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 DNFSB'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 DNFSB policies and Federal criteria, including, but not limited to, the following:

- *Government Auditing Standards* (April 2021).

[19] *Audit of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022* (Report No. DNFSB-22-A-07, issued September 29, 2022).

[20] *Independent Evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2021* (Report No. DNFSB-22-A-04, issued December 21, 2021).

[21] *Independent Evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020* (Report No. DNFSB-21-A-04, issued March 25, 2021).

[22] *Independent Evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2019* (Report No. DNFSB-20-A-05, issued March 31, 2020).

- 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).
- DNFSB*'s* policies and procedures, including but not limited to:
  - *DNFSB GSS System Security Plan (SSP)*
  - *DNFSB GSS Information System Contingency Plan (ISCP)*
  - *DNFSB Directive D-411.2 Information Systems Security Program*
  - *DNFSB GSS Continuous Monitoring Policies and Procedures Guide*
  - *DNFSB Risk Management Framework Handbook*
  - *DNFSB Risk Assessment Policy*
  - *DNFSB Supply Chain Risk Management Strategic Plan*
  - *DNFSB Operating Procedures OP-412.2-1 Vulnerability Management*
  - *DNFSB Configuration Management Policy*
  - *DNFSB Access Control Policy*
  - *DNFSB Security Awareness Training Policy*
  - *DNFSB Incident Response Process Guide Cyber Playbook*
  - *DNFSB Contingency Planning Policy*
  - *DNFSB Directive D-260.2 Privacy Program*
  - *DNFSB System and Communications Protection Policy*

We selected the DNFSB GSS information system from the total population of one DNFSB internal systems for testing. The DNFSB GSS is categorized as a moderate impact system, based on NIST FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*. We tested the DNFSB's GSS's 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.

STATUS OF PRIOR RECOMMENDATIONS

The table below summarizes the status of the open prior recommendations from the FY 2022 FISMA audit, FY 2021 FISMA evaluation, FY 2020 FISMA evaluation and FY 2019 FISMA evaluation.[23] At the time of testing and IG FISMA Reporting Metric submission, there remained 35 out of 56 open prior FISMA recommendations from the audit and evaluations referenced above. In March 1, 2023, DNFSB issued a memo on the *Status of DNFSB Open Audit Recommendations* to the DNFSB Office of the Inspector General (OIG) demonstrating their progress on audit recommendation remediation. 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 OIG's status of recommendation process.

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 1*: Implement a process to ensure a security control assessment for the DNFSB General Support System (GSS) is completed and documented on an annual basis.	This recommendation is resolved. DNFSB began an engagement in February 2023 and anticipates completing the external security assessment of the DNFSB GSS in Quarter 3 FY 2023.	Open At the time of our review, the security control assessment for the DNFSB GSS was not yet completed. Specifically, an annual security control assessment was not completed for FY 2021 – 2022 and was not completed for over nine months of FY 2023 (October 1, 2022 – June 30, 2023).
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 2*: Implement a process to validate the DNFSB GSS security authorization is maintained in accordance with DNFSB policy.	This recommendation is resolved. The *DNFSB Risk Management Framework Handbook* has been completed and approved.	Open The security authorization was expired as of

[23] See footnotes 19, 20, 21, and 23.

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
		Implementation proof will consist of external validation of system; DNFSB anticipates completing the external security assessment of the DNFSB GSS in Quarter 3 FY 2023.	November 8, 2018, and was not maintained in accordance with DNFSB policy. At the time of our review, an external security assessment to receive an updated authorization was not yet completed.
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 3*: Enforce existing DNFSB policy requirements to document security impact analyses, test plans, test results and backout plan requirements for each change.	DNFSB requests closure of this recommendation.	Closed For a sample of ten changes from the population of 67 changes from October 1, 2022, to February 13, 2023, no exceptions were noted related to the enforcement of existing DNFSB policy requirements to document security impact analyses, test plans, test results and backout plan requirements for each change as applicable.
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 4*: Complete the implementation and consistent performance of monthly reviews to ensure security impact	DNFSB requests closure of this recommendation.	Closed Quarterly reviews were

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
	analyses, test plans, and backouts plans are documented as required for each change.		implemented in place of the recommended monthly reviews; however, verified that reviews to ensure change requirements are met were performed.
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 5*: Complete the implementation of the configuration management training program and provide periodic refreshers to ensure evidence requirements are captured for change tickets.	DNFSB requests closure of this recommendation. DNFSB required all members of the IT team that are authorized to submit change request tickets to take remedial "CCB and Change Request Training" in August 2022 and then take an updated remedial training in December 2022 that addressed changes to the Change Control Board and Security Impact Analysis form process.	Open Specific evidence of a dedicated configuration management training program was not provided; however, we noted that change tickets sampled for testing were more consistent overall in compliance with policy requirements and a quarterly requirement review was implemented to reinforce, monitor for and remediate as needed any potential gaps in change policy compliance.
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 6*: Update the current change process, the Track-It! Tool or both to enforce segregation of duties controls for a requestor and an approver of a change	DNFSB requests closure of this recommendation.	Closed For a sample ten changes from the

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
	(e.g., requiring a second approver signature for all non-emergency changes, when the requester is eligible to be an approver).		population of 67 changes from October 1, 2022, to February 13, 2023, we noted that all Track-It! tickets sampled for testing required multiple configuration control board approvers (i.e., three) to vote to approve a change.
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 7*: Create procedures for vulnerability and compliance management based on risk and level of effort involved to mitigate confirmed vulnerabilities case-by-case such as: a. Prioritizing mitigation in accordance with all requirements specified by CISA BOD 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities and Emergency Directives, as applicable. b. Opening plans of action and milestones to track critical and high vulnerabilities that cannot be addressed within 30 days. c. Preparing risk-based decisions in unusual circumstances when there is a technical or cost limitation making mitigation of a critical or high vulnerability infeasible with documented, effective compensating controls coupled with a clear timeframe for planned remediation.	DNFSB published OP 412.2-1, Vulnerability Management Operating Procedures, on 2/21/23. DNFSB considers Recommendation 2022-7 to be fully remediated. DNFSB requests closure of this Recommendation.	Open DNFSB continues not to remediate identified critical and high vulnerabilities in accordance with timeframes required by DNFSB policy.

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 8*: Implement a solution to gradually automate, orchestrate, and centralize patching for each device.	DNFSB requests closure of this recommendation.	Closed The OIG reviewed the update rings, iOS update and compliance policies, a report of the current compliance status of DNFSB iPhones, and an example of the email sent to users of non-compliant phones.
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 9*: Develop and implement a data consistency and quality plan or similar procedure to help test and monitor data accuracy and quality of information coming from their implementation of Continuous Diagnostics and Mitigation (CDM).	DNFSB requests closure of this recommendation.	Closed The OIG reviewed screenshots from Qualys, a Weekly Vulnerability Report, and emails from the DNFSB to CDM to remediate discrepancies in the Qualys data and the CDM dashboard data.
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 10*: We recommend DNFSB management document and implement system and information integrity and systems and communications protection policies and procedures in accordance with DNFSB policy.	DNFSB requests closure of this recommendation.	Closed Inspected system and information integrity (SI) and systems and communications protection (SC) policies and noted that DNFSB documented and

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			implemented them in accordance with DNFSB policy.
DNFSB-22-A-07 FY 2022 FISMA Audit	*FY 2022 Recommendation 11*: We recommend that DNFSB management documents and implements a process to validate that the DNFSB GSS Information System Contingency Plan (ISCP) is tested annually, and any issues discovered during the contingency plan test are remediated timely.	DNFSB requests closure of this recommendation.	Closed Inspected the Contingency Planning Policy and noted that DNFSB management has documented requirements to test the ISCP annually with correction of any identified issues timely. Also verified that DNFSB management has also created a new process for performing and documenting restoration testing of the DNFSB GSS ISCP.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 1*: Update the Information Security Architecture (ISA) and use the updated ISA to: a. Assess enterprise, business process, and information system level risks; and b. Update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 4.	Open Remains a work in progress. See DNFSB's estimated target completion date.

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 2*: Using the results of recommendations one above: a. Utilizing guidance from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55 (Rev. 1) – *Performance Measurement Guide for Information Security* to establish performance metrics to manage and optimize all domains of the DNFSB information security program more effectively; b. Implement a centralized view of risk across the organization; and c. Implement formal procedures for prioritizing and tracking Plans of Action and Milestones (POA&Ms) to remediate vulnerabilities.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 4.	Open DNFSB has not completed addressing the related, dependent recommendation above. Also, see DNFSB's estimated target completion date.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 3*: Update the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, to include: a. Defining a frequency for conducting Risk Assessments to periodically assess agency risks to integrate results of the assessment to improve upon mission and business processes.	DNFSB requests closure of this recommendation.	Open The *DNFSB Risk Management Framework Handbook* does not define a frequency for conducting Risk Assessments to periodically assess agency risks to integrate results of the assessment to improve upon mission and business processes.

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			Note: The DNFSB Risk Assessment Policy approved 1/18/2023 documents a frequency; however, policy guidance on risk assessment performance is inconsistent and is not followed (i.e., no updated risk assessment or control assessment for the GSS).
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 4*: Define a Supply Chain Risk Management strategy to drive the development and implementation of policies and procedures for: a. How supply chain risks are to be managed across the agency; b. How monitoring of external providers compliance with defined cybersecurity and supply chain requirements; and c. How counterfeit components are prevented from entering the DNFSB supply chain.	DNFSB requests closure of this recommendation.	Open DNFSB did not define a Supply Chain Risk Management strategy to drive the development and implementation of policies and procedures for items a-c.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 5*: Conduct remedial training to re-enforce requirements for documenting security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.	DNFSB requests closure of this recommendation.	Open Although we noted an improvement in change documentation for our sampled changes, DNFSB did

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			not provide evidence supporting the development and delivery of remedial training for all members of the IT staff to re-enforce requirements for documenting security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 6*: Integrate the Configuration Management Plan with risk management and continuous monitoring programs and utilize lessons learned to make improvements to this plan.	DNFSB requests closure of this recommendation.	Closed Inspected the *DNFSB Risk Management Framework Handbook*, *DNFSB Risk Assessment Policy*, and the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* to determine aspects of configuration management (e.g., baseline compliance, patching, change control, etc.) are integrated with risk

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			management and continuous monitoring programs.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 7*: Implement automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.	DNFSB has procedures in place to automate the process of identifying privileged accounts that are inactive but wants to have a formal approval process for disabling or deleting privileged accounts; given the small number of privileged users at the DNFSB, this is an acceptable risk. DNFSB will request a risk acceptance for this recommendation by Quarter 3 FY 2023.	Open DNFSB will request a risk acceptance for this recommendation.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 8*: Continue efforts to implement data loss prevention functionality for the Microsoft Office 365 environment.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 3.	Open In the Status of Open Recommendations provided by DNFSB, noted that the IT team will continue to work with the Records Management staff in the Division of Operational Services to better define the data loss prevention policies in DNFSB's Office 365 tenant.

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 9*: Update agency strategic planning documents to include clear milestones for implementing strong authentication, the Federal Identity, Credential, and Access Management (ICAM) architecture and Office of Management and Budget (OMB) Memorandum (M)-19-17, and phase 2 of DHS's CDM program.	This recommendation remains open. Estimated target completion date: No estimated completion date available until CDM finalizes their ICAM service offerings.	Open Please refer to DNFSB's Status.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 10*: Conduct the agency's annual breach response plan exercise for FY 2021.	DNFSB requests closure of this recommendation.	Open This recommendation has been overcome by current events (i.e., conducting the exercise for FY 2021). However, evidence of a more recent breach response plan exercise was not provided. Also, inspected the incident response and contingency planning exercises completed and noted they did not include an evaluation of the breach response plan.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 11*: Continue efforts to develop and implement role-based privacy training for users with significant privacy or data protection related duties.	DNFSB requests closure of this recommendation.	Open In reply to *Status of Recommendations: Independent Evaluation of the DNFSB's*

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			Implementation of the Federal Information Security Modernization Act of 2014 For Fiscal Year 2021 (DNFSB-22-A-04), DNFSB management stated: "In addition, dedicated Annual Privacy Act Training was given to all DNFSB users in August & September 2021 and is being given again in August & September of 2022." However, upon inspection of the training records provided, evidence of all DNFSB users completing Privacy Act Training was not provided and specific role-based training was not called out either.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 12*: Formally document requirements and procedures for completion of role-based training and enforcement methods for individuals who do not complete role-based training.	DNFSB requests closure of this recommendation. DNFSB published its "Security Awareness Training Policy" in August 2022 that contains requirements for role-based	Closed The *Security Awareness Training Policy* formally documents the requirements and

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
		training and enforcement actions for individuals that do not complete required role-based training.	procedures for completion of role-based training and enforcement methods for individuals that do not complete it.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 13*: Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.	This recommendation is resolved. DNFSB began an engagement in February 2023 and anticipates completing the external security assessment of the DNFSB GSS in Quarter 3 FY 2023.	Open Progress has been made in refining procedures such as the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* to support adoption of an ongoing authorization model. However, ongoing authorization of the DNFSB GSS is not yet in place. Specifically, the last traditional ATO lasted for three years from the date of signature, expiring November 8, 2018. Also, at the time of our review, an external security assessment to receive an updated authorization was not yet completed.

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 14*: Update the DNFSB Information Security Continuous Monitoring (ISCM) policies and procedures clearly defining what needs to be monitored at the system and organization level.	DNFSB requests closure of this recommendation.	Closed Inspected the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* and the *DNFSB Risk Management Framework Handbook* and noted that DFNSB has updated its policies and procedures to clearly define what needs to be monitored at the system and organization level.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 15*: Define standard operating procedures for the use of the agency's continuous monitoring tools or update the continuous monitoring plan to include the use of new monitoring tools.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 4.	Closed Inspected the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* to determine the use of the agency's continuous monitoring tools is documented.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 16*: Defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program.	DNFSB requests closure of this recommendation.	Closed Inspected the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* and

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			noted that DNFSB has defined qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program in Appendix C Continuous Monitoring Reports.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 17*: Define handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents.	DNFSB requests closure of this recommendation.	Closed Inspected the *DNFSB Incident Response Process Guide Cyber Playbook* and noted that DNFSB has defined handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents.

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 18*: Consistently test the incident response plan annually.	DNFSB requests closure of this recommendation.	Closed DNFSB tested the incident response plan through a tabletop exercise on May 24-25 and produced evidence of lessons learned in the Hotwash section of the exercise report.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 19*: Update the Agency's incident response plan to reflect United States Computer Emergency Readiness Team (US CERT) incident reporting guidelines.	DNFSB requests closure of this recommendation.	Closed Inspected the *DNFSB Incident Response Plan* to determine DNFSB's process for analyzing, documenting, and reporting security incidents is based on US-CERT guidelines.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 20*: Allocate and train staff with significant incident response responsibilities.	DNFSB requests closure of this recommendation.	Open Inspected the DNFSB GSS System Security Plan (SSP) Incident Response (IR)-2 Incident Response Training security control implementation details to determine: "Currently the DNFSB

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			is reviewing incident response training options to select a fitting option. Once complete, this control will be implemented." Also inspected the *DNFSB GSS Incident Response Plan* and *DNFSB Incident Response Process Guide Cyber Playbook* to determine incident response training was not covered in detail.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 21*: Configure all incident response tools in place to be interoperable, can collect and retain relevant and meaningful data that is consistent with the incident response policy, plans and procedures.	DNFSB requests closure of this recommendation.	Closed Inspected the SIEM tool configuration and determined it is interoperable with other incident response tools in place.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 22*: Develop and track metrics related to the performance of contingency planning and recovery related activities.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 3.	Open Evidence supporting implementation of metrics related to performance of contingency planning and recovery related activities was not

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			provided. Examples include: • Establish qualitative or quantitative metrics/dashboards to ensure the effectiveness of the contingency planning. (e.g., up-to-date business impact analysis with functional recovery exercise measuring whether established recovery point and time objectives were met). • Evidence of use of performance metrics/dashboards • Evidence of verification and validation of data feeding the metrics/dashboard.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 23*: Conduct a business impact assessment within every two years to assess mission essential functions and incorporate the results into strategy and mitigation planning activities.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 2.	Open DNFSB has not conducted an annual Business Impact Assessment of its GSS. The last BIA

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			was conducted in FY 2018.
DNFSB-22-A-04 FY 2021 FISMA Evaluation	*FY 2021 Recommendation 24*: Implement role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 2.	Open Although the DNFSB Contingency Planning Policy requires the provision of training and although testing was conducted during the audit period for two exercises, evidence of the implementation and completion of role-based training for individuals with significant contingency planning and disaster recovery related responsibilities was not provided.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 1:* Define an ISA in accordance with the Federal Enterprise Architecture Framework.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 4.	Open Remains a work in progress. See DNFSB's estimated target completion date.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 2:* Use the fully defined ISA to: a. Assess enterprise, business process, and information system level risks; b. Formally define enterprise, business process, and information system level risk	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 4.	Open Remains a work in progress. See DNFSB's estimated target completion date.

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
	tolerance and appetite levels necessary for prioritizing and guiding risk management decisions; c. Conduct an organization wide security and privacy risk assessment; and d. Conduct a supply chain risk assessment.		
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 3:* Using the results of recommendations one (1) and two (2) above: a. Collaborate with the DNFSB's Cybersecurity Team to establish performance metrics in service level agreements to measure, report on, and monitor the risks related to contractor systems and services being monitored by IT Operations; b. Utilize guidance from the NIST SP 800-55 (Rev. 1) – *Performance Measurement Guide for Information Security* to establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program; c. Implement a centralized view of risk across the organization; and d. Implement formal procedures for prioritizing and tracking POA&M to remediate vulnerabilities.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 4.	Open Remains a work in progress. See DNFSB's estimated target completion date.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 4:* Finalize the implementation of a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in near real time. Continue ongoing efforts to apply	DNFSB requests closure of this recommendation. Only iPhones purchased through Apple Business Manager program can be enrolled in Intune, so no	Open Evidence of detection of unauthorized hardware and of the capability to deny

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
	the Track-It!, ForeScout, and KACE solutions.	unauthorized mobile hardware can connect to DNFSB's IT resources. Users cannot install unauthorized software (all software on iPhones must be approved and installed through Intune; users cannot access the Apple App Store).	access to agency enterprise services when security and operating system updates have not been applied for mobile devices within a given period based on agency policy or guidance was not provided.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 5:* Conduct remedial training to re-enforce requirements for documenting Change Control Board's (CCB's) approvals and security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.	DNFSB requests closure of this recommendation. DNFSB required all members of the IT team that are authorized to submit change request tickets to take remedial "CCB and Change Request Training" in August 2022 and then take an updated remedial training in December 2022 that addressed changes to the Change Control Board and Security Impact Analysis form process.	Open Although we noted an improvement in change documentation for our sampled changes, DNFSB did not provide evidence supporting the development and delivery of remedial training for all members of the IT staff to re-enforce requirements for documenting CCB's approvals and security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			Management Plan.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 6:* Implement procedures and define roles for reviewing configuration change activities to the DNFSB's information system production environment by those with privileged access to verify the activity was approved by the system CCB and executed appropriately.	DNFSB requests closure of this recommendation.	Closed Inspected the *DNFSB Configuration Management Policy* and determined it documents roles/responsibilities for reviewing configuration change activities and stipulates approvals required for each requested change. Also, for a sample of ten changes from the population of 67 changes from October 1, 2022, to February 13, 2023, noted that all sampled changes were approved by the CCB and executed as appropriate in accordance with the *DNFSB Configuration Management Policy*.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 7:* Implement a technical capability to restrict new employees and contractors from being granted access to the DNFSB's systems and information until a non-disclosure agreement	DNFSB requests closure of this recommendation.	Open Evidence supporting implementation of the technical capability

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
	is signed and uploaded to a centralized tracking system.		restricting granting of access until after a non-disclosure agreement is signed and uploaded was not provided. Also, for a sample of six non-privileged users from the population of 17 created since October 1, 2022, we noted: • For one new user, the agreements were signed after access was provisioned. • For two of the new users, we were unable to verify when the agreements were signed as they did not include the date next to the wet signatures / were not digital signatures with a date/timestamp.
DNFSB-21-A-04 FY 2020 FISMA	*FY 2020 Recommendation 8:* Implement the technical capability to require	DNFSB requests closure of this recommendation.	Closed

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
Evaluation	Personal Identity Verification (PIV) or Identification and Authentication Level of Assurance (IAL) 3 to all DNFSB privileged accounts.		Inspected multifactor authentication configuration settings and determined that DNFSB has implemented strong authentication mechanisms to authenticate to applicable organizational systems and facilities, such as PIV and Windows Hello.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 9:* Implement automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.	DNFSB will request a risk acceptance for this recommendation by Quarter 3 FY 2023.	Open DNFSB will request a risk acceptance for this recommendation.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 10:* Continue efforts to develop and implement role-based privacy training.	DNFSB requests closure of this recommendation.	Open Upon inspection of the training records provided, evidence of all DNFSB users completing Privacy Act Training was not provided and specific role-based privacy training was not called out either.

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 11:* Conduct the agency's annual breach response plan exercise for FY 2021.	DNFSB requests closure of this recommendation.	Open Inspected the incident response and contingency planning exercises completed and noted they did not include an evaluation of the breach response plan.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 12:* Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.	DNFSB requests closure of this recommendation.	Open Progress has been made in refining procedures such as the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* to support adoption of an ongoing authorization model. However, ongoing authorization of the DNFSB GSS is not yet in place. Specifically, the last traditional ATO lasted for three years from the date of signature, expiring November 8, 2018. Also, at the time of our review, an external security

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			assessment to receive an updated authorization was not yet completed.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 13:* Update the DNFSB's incident response plan to include profiling techniques for identifying incidents and strategies to contain all types of major incidents.	DNFSB requests closure of this recommendation.	Closed Inspected the *DNFSB Incident Response Process Guide Cyber Playbook* and determined it includes profiling techniques for incident identification and strategies for containing them.
DNFSB-21-A-04 FY 2020 FISMA Evaluation	*FY 2020 Recommendation 14:* Based on the results of the DNFSB's supply chain risk assessment included in the recommendation for the Identify function above, update the DNFSB's contingency planning policies and procedures to address Information and Communications Technology (ICT) supply chain risk.	This recommendation remains open. Estimated target completion date: Quarter 4 FY 2023.	Open ICT supply chain risk was not addressed in DNFSB's contingency planning policies and procedures, Supply Chain Risk Management Strategic Plan or in the DNFSB GSS SSP.
DNFSB-20-A-05 FY2019 FISMA Evaluation	*FY 2019 Recommendation 3:* Using the results of recommendations one (1) and two (2) above: a. Implement an automated solution to help maintain an up-to-date, complete, accurate, and readily available Agency-wide view of the security configurations	DNFSB requests closure of this recommendation.	Open DNFSB has not completed the recommended items. See respective conclusions

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
	for all its GSS components; Cybersecurity Team exports metrics and vulnerability reports and sends them to the Chief Information Security Officer (CISO) and Chief Information Officer (CIO)'s Office monthly for review. Develop a centralized dashboard that Cybersecurity Team and the CISO can populate for real-time assessments of compliance and security policies. b. Collaborate with DNFSB Cybersecurity Team Support to establish performance metrics in service level agreements to measure, report on, and monitor the risks related to contractor systems and services being monitored by Cybersecurity Team. c. Establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program. d. Implement a centralized view of risk across the organization.		documented in FY 2021 Recommendation 2 and FY 2020 Recommendation 3 above. As noted in those related prior year recommendations, DNFSB anticipates completing these tasks by Quarter 4 FY 2023.
DNFSB-20-A-05 FY2019 FISMA Evaluation	*FY 2019 Recommendation 5:* Management should re-enforce requirements for performing DNFSB's change control procedures in accordance with the agency's Configuration Management Plan by defining consequences for not following these procedures and conducting remedial training as necessary.	DNFSB requests closure of this recommendation. DNFSB required all members of the IT team that are authorized to submit change request tickets to take remedial "CCB and Change Request Training" in August 2022 and then take an updated remedial training in December 2022 that	Open Neither the *DNFSB Configuration Management Policy* nor the DNFSB GSS SSP security control implementation details for Configuration Management (CM)

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
		addressed changes to the Change Control Board and Security Impact Analysis form process. DNFSB's User Agreement/Rules of Behavior form that all users are required to sign includes the language "I understand that non-compliance with the DNFSB's directives and policies may be cause for disciplinary action up to and including system privilege revocation, dismissal from the DNFSB or removal from contract, and criminal and/or civil penalties."	family controls define consequences for not adhering to change control requirements or reflect details about conduct of remedial training as necessary for change control requirement reinforcement. Additionally, DNFSB did not provide evidence supporting the completion of configuration management training.
DNFSB-20-A-05 FY2019 FISMA Evaluation	*FY 2019 Recommendation 7:* Complete and document a risk-based justification for not implementing an automated solution (e.g., Splunk) to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network.	DNFSB requests closure of this recommendation.	Closed Inspected evidence supporting the implementation of a suite of automated solutions and determined that a view of security configurations for information system components connected to DNFSB's network is now in place.
DNFSB-20-A-05 FY2019 FISMA	*FY 2019 Recommendation 8:* Continue efforts to meet milestones of the	DNFSB requests closure of this recommendation.	Open

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
Evaluation	DNFSB ICAM Strategy necessary for fully transitioning to DNFSB's "to-be" ICAM architecture.		DNFSB has continued efforts to meet milestones in its ICAM strategy and has begun the effort to adopt zero trust architecture as it transitions towards its "to-be" architecture.
DNFSB-20-A-05 FY2019 FISMA Evaluation	*FY 2019 Recommendation 9:* Complete current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.	DNFSB requests closure of this recommendation.	Open Progress has been made in refining procedures such as the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* to support adoption of an ongoing authorization model. However, ongoing authorization of the DNFSB GSS is not yet in place. Specifically, the last traditional ATO lasted for three years from the date of signature, expiring November 8, 2018. Also, at the time of our review, an external security assessment to receive

Defense Nuclear Facilities Safety Board
FY 2023 Audit of the DNFSB's Implementation of the FISMA

Report No.	Recommendation	DNFSB's Status	Auditor's Position on Status
			an updated authorization was not yet completed.
DNFSB-20-A-05 FY2019 FISMA Evaluation	*FY 2019 Recommendation 10:* Identify and fully define requirements for the incident response technologies DNFSB plans to utilize in the specified areas and how these technologies respond to detected threats (e.g., cross-site scripting, phishing attempts, etc.).	DNFSB requests closure of this recommendation.	Closed Inspected the *DNFSB Incident Response Process Guide Cyber Playbook* and determined requirements for incident response technologies are specified in conjunction with how they will be used to respond to detected threats.
DNFSB-20-A-05 FY2019 FISMA Evaluation	*FY 2019 Recommendation 11:* Based on the results of DNFSB's supply chain risk assessment included in the recommendation for the Identify function above, update DNFSB's contingency planning policies and procedures to address ICT supply chain risk.	DNFSB requests closure of this recommendation.	Open ICT supply chain risk was not addressed in DNFSB's contingency planning policies and procedures, Supply Chain Risk Management Strategic Plan or in the DNFSB GSS SSP.

DNFSB's MANAGEMENT COMMENTS

DEFENSE NUCLEAR FACILITIES
SAFETY BOARD
Washington, DC 20004-2901

September 8, 2023

TO: Hruta Virkar
Assistant Inspector General for Audits
Office of the Inspector General

FROM: Katherine Herrera
Acting Executive Director of Operations
Defense Nuclear Facilities Safety Board

RE: DNFSB Management Comments
Audit of the Defense Nuclear Facilities Safety Board's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023

The DNFSB continues its efforts to improve its information security program and to fully comply with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA), Executive Orders, Memoranda from the Office of Management and Budget, Emergency Directives and Binding Operational Directives from the Cybersecurity and Infrastructure Security Agency, and guidance from the National Institute of Standards and Technology.

The DNFSB agrees with the Office of the Inspector General's (OIG) assessment of the current state of its information security program, as reflected in the FY 2023 IG Metrics and this FY 2023 Audit of the DNFSB's Implementation of the FISMA. The DNFSB would also like to take this opportunity to capture all of the actions that DNFSB has taken to resolve and close Recommendations from prior year FISMA audits or to improve its information technology systems, environment, and governance.

The OIG's FY 2023 FISMA Audit recognizes that DNFSB took actions that were sufficient to close 21 prior year Recommendations – that is more recommendations closed than in the prior three years combined. DNFSB submitted two memos to the OIG in August of 2022 with explanations of actions taken and requesting the closure of 14 open Recommendations, 8 of which were not closed during the FY 2023 Audit. The OIG has informed DNFSB that the remaining 8 Recommendations were not closed because the evidence required to verify the closure of the Recommendations was not provided during the timeframe of the FY23 audit fieldwork. DNFSB looks forward to the closure of these 8 additional Recommendations.

The DNFSB appreciates the cyber security review conducted by the OIG. With the ultimate goal being information technology systems that are resilient against cyber intrusions and unauthorized exfiltration or interception of data, the OIG continues to be a partner with us as an objective third-party reviewer of our compliance with government-wide cyber security requirements.