



MEMORANDUM

DATE: September 29, 2022

TO: James Biggins
Acting Executive Director of Operations

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

SUBJECT: AUDIT OF THE DNFSB'S IMPLEMENTATION OF THE
FEDERAL INFORMATION SECURITY MODERNIZATION
ACT OF 2014 FOR FISCAL YEAR 2022 (DNFSB-22-A-07)

The Office of the Inspector General (OIG) contracted with CliftonLarsonAllen LLP (CLA) to conduct an independent audit of the Defense Nuclear Facilities Safety Board's (DNFSB) Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2022. Attached is CLA's report titled *Audit of the DNFSB'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 DNFSB. The findings and conclusions presented in this report are the responsibility of CLA. The OIG's responsibility is to provide adequate 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 the DNFSB did not establish an effective agency-wide information security program, and there are 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.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions, please call me at (301) 415-1982 or Terri Cooper, Team Leader at (301) 415-5965.

Attachment: As stated

**Audit of the Defense Nuclear Facilities Safety Board'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
Defense Nuclear Facilities Safety Board
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 Defense Nuclear Facilities Safety Board's (DNFSB) 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 DNFSB. We will be pleased to discuss any questions you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal



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) 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 (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 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, IGs were required 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.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 April to July 2022. The audit covered the period from October 1, 2021, through July 30, 2022.

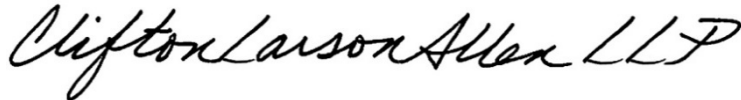
We concluded that the DNFSB did not implement effective information security policies, procedures and practices, since it achieved an overall *Level 3 – Consistently Implemented* maturity level; and therefore the DNFSB did not have an effective information security program. We noted weaknesses in the risk management, configuration management, data protection and privacy, information security continuous monitoring, and contingency planning domains of the FY 2022 IG FISMA Reporting Metrics. As a result, we made 11 new recommendations to assist the DNFSB in strengthening its information security program. Additionally, 22 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 DNFSB 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 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

A handwritten signature in black ink that reads "CliftonLarsonAllen LLP". The signature is written in a cursive, flowing style.

Arlington, Virginia
September 28, 2022

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

Table of Contents

EXECUTIVE SUMMARY	1
Audit Results	2
AUDIT FINDINGS	5
1. Weaknesses with Security Assessment and Authorization Process	5
2. Weaknesses in Configuration Management Process related to System Changes.....	6
3. Weaknesses in the Vulnerability Management Program.....	7
4. Weaknesses in Documenting and Implementing System and Information Integrity and Systems and Communications Protection Policies.....	9
5. Weakness in Information System Contingency Plan Testing.....	10
APPENDIX I: BACKGROUND.....	12
APPENDIX II: OBJECTIVE, SCOPE, AND METHODOLOGY.....	15
APPENDIX III: STATUS OF PRIOR RECOMMENDATIONS.....	18
APPENDIX IV: DNFSB'S MANAGEMENT COMMENTS.....	23

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

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 6, 2021, the OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete IG FISMA Reporting Metrics² to independently assess their agencies' information security program. The OMB selected a core group of 20 metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will be evaluated in metrics on a two-year cycle. In addition, the OMB 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.

For this year's review, IGs were required by the OMB 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.³ 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 mapped to the FY 2022 Core IG FISMA Reporting Metrics for the DNFSB General Support System (GSS).

² We submitted our responses to the FY 2022 Core Metrics to DNFSB OIG as a separate deliverable under the contract for this audit.

³ The function areas are further broken down into nine domains.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

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.

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.⁴ 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 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 3: Consistently Implemented	Risk Management	Level 3: Consistently Implemented
		Supply Chain Risk Management	Level 1: Ad-Hoc
Protect	Level 4: Managed and Measurable	Configuration Management	Level 3: Consistently Implemented
		Identity and Access Management	Level 4: Managed and Measurable
		Data Protection and Privacy	Level 4: Managed and Measurable
		Security Training	Level 4: Managed and Measurable
Detect	Level 2: Defined	Information Security Continuous Monitoring	Level 2: Defined
Respond	Level 2: Defined	Incident Response	Level 2: Defined
Recover	Level 3: Consistently Implemented	Contingency Planning	Level 3: Consistently Implemented
Overall	Level 3: Consistently Implemented – Not Effective		

⁴ In the FY 2021 FISMA evaluation, the results were based on 66 metric questions. The FY 2022 FISMA audit results are based on 20 metric questions.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

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

- The DNFSB's size, complexity, and environment were taken into consideration at both the individual metric level, and the domain level; and in several cases, the control environment was taken into consideration and the individual metric level was raised.
- The OMB considers the 20 Core Metrics to be the most critical to determine the effectiveness of an Agency's information security program. Therefore, the audit was focused around the 20 Core Metrics.
- The DNFSB has a significant number of open prior year recommendations. Since last year, the agency demonstrated actions to close two of the 24 open prior FISMA recommendations. In addition, there were prior year recommendations with significant impact to the Core 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.

While the DNFSB's security program did not reach an effective level, the DNFSB continues to stress its commitment to improving information security throughout the agency. Specifically, DNFSB has implemented multi-factor authentication for user access; established controls for protecting personally identifiable information; and updated its Incident Response Plan to reflect United States Computer Emergency Readiness Team (US-CERT) reporting guidelines.

However, to fully progress towards "Managed and Measurable", the DNFSB will need to address weaknesses in its security program related to the risk management, configuration management, data protection and privacy, information security continuous monitoring, and contingency planning domains of the FY 2022 Core IG FISMA Reporting Metrics (see **Table 2** below). As a result of the weaknesses noted, we made 11 new recommendations to assist the DNFSB in strengthening its information security program. Additionally, we noted 22 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	Weaknesses with Security Assessment and Authorization Process (Finding 1)
	Supply Chain Risk Management	No weaknesses noted.
Protect	Configuration Management	Weaknesses in Configuration Management Process related to System Changes (Finding 2)

⁵ See appendix III for status of prior year recommendations.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

Cybersecurity Framework Security Function	FY 2022 Core IG FISMA Reporting Metrics Domain	Weaknesses Noted
		Weaknesses in the Vulnerability Management Program (Finding 3)
	Identity and Access Management	No weaknesses noted.
	Data Protection and Privacy	Weaknesses in Documenting and Implementing System and Information Integrity and Systems and Communications Protection Policies (Finding 4)
	Security Training	No weaknesses noted.
Detect	Information Security Continuous Monitoring	Weaknesses with Security Assessment and Authorization Process (Finding 1)
Respond	Incident Response	No weaknesses noted.
Recover	Contingency Planning	Weakness in Information System Contingency Plan Testing (Finding 5)

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 with Security Assessment and Authorization Process

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

The DNFSB did not conduct security control assessments annually for the general support system (GSS) in accordance with DNFSB policy. Specifically, a security control assessment was last conducted in 2020. Additionally, a current authorization to operate (ATO) for the DNFSB GSS was not maintained. The ATO expired on November 8, 2021.

The DNFSB is in the process of working with the Department of the Interior to perform a security control assessment via an interagency agreement, pending availability of funds.

DNFSB GSS System Security Plan (SSP), dated May 2022, implementation details and organizationally defined values for the following security controls state, in part:

CA-2: Control Assessment
Control:

...

- b. Develop a control assessment plan that describes the scope of the assessment including:
 - 1. Controls and control enhancements under assessment;
 - 2. Assessment procedures to be used to determine control effectiveness; and
 - 3. Assessment environment, assessment team, and assessment roles and responsibilities;
- c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
- d. Assess the controls in the system and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
- e. Produce a control assessment report that documents the results of the assessment; and
- f. Provide the results of the control assessment to Authorizing Official, System Owner, Information Technology Staff.

CA-6: Security Authorization
Control:

...

- c. Ensure that the authorizing official for the system, before commencing operations:
 - 1. Accepts the use of common controls inherited by the system; and
 - 2. Authorizes the system to operate;

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

- d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
- e. Updates the authorizations annually.

Without conducting annual security control assessments and maintaining current ATOs, DNFSB is at risk of being unaware of the current weaknesses and risks to its information system environment.

We recommend that DNFSB's Chief Information Security Officer:

Recommendation 1: Implement a process to ensure a security control assessment for the DNFSB GSS is completed and documented on an annual basis.

Recommendation 2: Implement a process to validate the DNFSB GSS security authorization is maintained in accordance with DNFSB policy.

2. Weaknesses in Configuration Management Process related to System Changes

Cybersecurity Framework Security Function: *Protect*

FY 2022 Core IG FISMA Reporting Metrics Domain: *Configuration Management*

We were unable to validate whether backout plans, system impact analyses, and testing was completed for a sample of 17 system changes from total population of 169 system changes. Specifically, we noted the following:

- Three sampled changes did not have documented backout plans.
- Three sampled changes did not have documented security impact analyses.
- Three sampled changes did not have documented security impact analyses and backout plans.
- One sampled change did not have a documented security impact analysis, test plan, test results and backout plan.
- One sampled change was approved by the requester.

These issues occurred because the Track-It! application⁶ did not have configuration settings enforced for all requirements of its change process. Additionally, there was not a training program in place at the time of our review to ensure specific forms of evidence required for each change request are paired with each ticket. Further, the system did not require a second approver signature when a senior official, such as the Chief Information Security Officer, requests a change.

DNFSB GSS SSP, dated May 2022, the implementation details and organizationally defined values for the following security control states, in part:

CM-3: Configuration Change Control
Control:

...

⁶ Track-It! is an IT service desk management platform that handles change management processes.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

- b. Reviews proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
- c. Document configuration change decisions associated with the system;
- d. Implement approved configuration-controlled changes to the system;
- e. Retain records of configuration-controlled changes to the system for indefinitely;
- f. Monitor and review activities associated with configuration-controlled changes to the system; and
- g. Coordinate and provide oversight for configuration change control activities through Configuration Change Board (CCB) that convenes periodically.

Without documenting security impact analyses, testing and backout plans, the DNFSB is at risk of being unaware of the security impact and risks caused by changes to its information system environment. In addition, there is an increased risk of unauthorized changes without segregation of duties controls for a requestor and an approver of a change.

We recommend that DNFSB's Chief Information Security Officer:

Recommendation 3: Enforce existing DNFSB policy requirements to document security impact analyses, test plans, test results and backout plan requirements for each change.

Recommendation 4: Complete the implementation and consistent performance of monthly reviews to ensure security impact analyses, test plans, test results and backout plans are documented as required for each change.

Recommendation 5: Complete the implementation of the configuration management training program and provide periodic refreshers to ensure evidence requirements are captured for change tickets.

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 (e.g., requiring a second approver signature for all non-emergency changes, when the requester is eligible to be an approver).

3. Weaknesses in the Vulnerability Management Program

Cybersecurity Framework Security Function: Protect
FY 2022 Core IG FISMA Reporting Metrics Domain: Configuration Management

The DNFSB did not resolve critical and high-risk vulnerabilities within 30 days, as required by DNFSB policy.

The vulnerability timeframes were not met consistently because patching is done individually for each device (e.g., peripheral) through each web interface manually. Additionally, the Continuous Diagnostics and Mitigation (CDM) application was not providing DNFSB with accurate data of the current number of open vulnerabilities.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

DNFSB GSS SSP, dated May 2022, implementation details and organizationally defined values for the following security controls state:

SI-2 Flaw Remediation

The organization:

- a. Identifies, reports, and corrects information system flaws.

...

RA-5 Vulnerability Scanning

The organization:

- a. Scans for vulnerabilities in the information system and hosted applications daily and when new vulnerabilities potentially affecting the system/applications are identified and reported;

...

- d. Remediates legitimate vulnerabilities within 30 days in accordance with an organizational assessment of risk.

Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, dated November 3, 2021, states the following required actions:

1. Within 60 days of issuance, agencies shall review and update agency internal vulnerability management procedures in accordance with this Directive. If requested by CISA, agencies will provide a copy of these policies and procedures. At a minimum, agency policies must:
 - a. Establish a process for ongoing remediation of vulnerabilities that CISA identifies, through inclusion in the CISA-managed catalog of known exploited vulnerabilities, as carrying significant risk to the federal enterprise within a timeframe set by CISA pursuant to this directive;

...

 - e. Set internal tracking and reporting requirements to evaluate adherence with this Directive and provide reporting to CISA, as needed.
2. Remediate each vulnerability according to the timelines set forth in the CISA-managed vulnerability catalog.

A variety of critical vulnerabilities could be exploited using unsophisticated techniques to take control of systems, to cause a denial-of-service attack, or to allow unauthorized access to the DNFSB systems and applications. In addition, operating system and application software that is missing security patches or software for which the vendor no longer maintains updated security patches could leave security weaknesses unfixed, exposing those systems to increased attack methods compromising the confidentiality, integrity, and availability of data.

We recommend that DNFSB's Chief Information Security Officer:

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

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.*

Recommendation 8: *Implement a solution to gradually automate, orchestrate and centralize patching for each device.*

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 CDM.*

4. Weaknesses in Documenting and Implementing System and Information Integrity and Systems and Communications Protection Policies

Cybersecurity Framework Security Function: Protect

FY 2022 Core IG FISMA Reporting Metrics Domain: Data Protection and Privacy

The DNFSB had not documented systems and information integrity and systems and communications protection policies and procedures. The DNFSB management indicated that internal discussions need to be held to validate and formally document these requirements.

DNFSB GSS SSP, dated May 2022, implementation details and organizationally defined values for the following security controls state:

SI-1 Systems and Information Integrity Policy and Procedures

The organization:

- a. Develops, documents, and disseminates to: DNFSB IT Staff
 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
- b. Reviews and updates the current:
 1. System and information integrity policy yearly; and
 2. System and information integrity procedures yearly.

SC-1 System and Communications Protection Policy and Procedures

The organization:

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

- a. Develops, documents, and disseminates to DNFSB IT Staff
 - 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
- b. Reviews and updates the current:
 - 1. System and communications protection policy yearly; and
 - 2. System and communications protection procedures yearly.

Without documented policies and procedures, individual employees, contractors, or both may be unaware of requirements and their responsibilities for systems and information integrity and systems and communications protection.

We recommend that DNFSB's Chief Information Security Officer:

Recommendation 10: Document and implement system and information integrity and systems and communications protection policies and procedures in accordance with DNFSB policy.

5. Weakness in Information System Contingency Plan Testing

Cybersecurity Framework Security Function: Recover
FY 2022 Core IG FISMA Reporting Metrics Domain: Contingency Planning

The DNFSB GSS Information System Contingency Plan (ISCP) was not tested annually as required by DNFSB policy. The last contingency plan test was conducted in 2019.

DNFSB management stated that competing projects limited the capability to allocate resources to conduct a contingency plan test. In addition, management was placing reliance on participation in the Eagle Horizon exercise and conduct of routine operations related to restoration of backups instead of completing the contingency plan test.

DNFSB GSS SSP, dated May 2022, implementation details and organizationally defined values for the following security controls state, in part:

CP-4 Contingency Plan Testing

The organization:

- a. Test the contingency plan for the information system annually using annual Federal Emergency Management Agency (FEMA) directed Continuity of Operations Plan (COOP) exercise to determine the effectiveness of the plan and the organizational readiness to execute the plan;
- b. Review the contingency plan test results; and
- c. Initiates corrective actions, if needed.

CP-2 Contingency Plan

The organization:

...

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

- g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training...

DNFSB GSS Information System Contingency Plan, dated May 2022, Section 9 Review and Testing the Disaster Recovery Plan, states:

The ISCP will be reviewed annually or as required to remain accurate and current. The developed ISCP will be tested for efficiency. Testing provides a platform where an analysis can be performed as to what changes if any are required and appropriate adjustments to the plan can be made. The Chief Information Officer will direct the scope and requirements of the testing on an annual basis.

Contingency plan testing helps to identify recovery weaknesses should a real event occur. Therefore, contingency plans that are not tested at least annually can risk the failure of the organization's operability of the plan and/or the plan's overall effectiveness. Loss of information system resources may lead to data loss and decreased staff productivity, and a prolonged outage may affect the DNFSBs' ability to perform its mission.

We recommend that DNFSB's Chief Information Security Officer:

Recommendation 11: Document and implement a process to validate that the DNFSB GSS ISCP is tested annually, and any issues discovered during the contingency plan test are remediated timely.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

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:⁷

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.

⁷ 44 USC § 3554, Federal agency responsibilities.

Defense Nuclear Facilities Safety Board FY 2022 Audit of the DNFSB's Implementation of the FISMA

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.

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 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 OMB, and where applicable, 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.⁸ 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, IGs 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**.

⁸ 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*.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB'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.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

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 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, IGs 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 DNFSB'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, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2022 Core 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 2021 FISMA evaluation.⁹

Audit fieldwork covered the DNFSB's headquarters located in Washington, D.C. from April to July 2022. The audit covered the period from October 1, 2021, through July 30, 2022.

⁹ *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).

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

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.¹⁰ 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:

- 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 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.
- 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).
- CISA BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- DNFSB's policies and procedures, including but not limited to:
 - *DNFSB GSS SSP*
 - *DNFSB GSS Information System Contingency Plan*

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*

¹⁰ Ibid. footnote 9.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

Information and Information Systems. We tested the DNFSB's GSS's 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.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

STATUS OF PRIOR RECOMMENDATIONS

The table below summarizes the status of the open prior recommendations from the FY 2021 FISMA evaluation.¹¹ At the time of testing and IG FISMA Reporting Metric submission, there remained 22 out of 24 open prior FISMA recommendations from the FY 2021 FISMA evaluation. On August 19, 2022, DNFSB issued a memo on the *Closure of FY 21 and FY 22 FISMA Audit Recommendations* to OIG demonstrating their progress on audit recommendation remediation. However, since remediation occurred after fieldwork and issuance of the IG FISMA Reporting Metrics, there has not been sufficient time to determine if the processes and controls implemented are now operating effectively. A follow-up on the open recommendations recorded in this report will occur during the next audit cycle.

Recommendation Number	Recommendation	DNFSB's Status	Auditor's Position on Status
1	Update the Information Security Architecture (ISA) and use the updated ISA to: a. Assess enterprise, business process, and information system level risks; 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 1.	Open
2	Using the results of recommendations one above: a. Utilizing guidance from the NIST SP 800-55 Rev. 1 <i>Performance Measurement Guide for Information Security</i> 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; 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

¹¹ Ibid. footnote 9.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

Recommendation Number	Recommendation	DNFSB's Status	Auditor's Position on Status
3	<p>Update the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, to include:</p> <p>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.</p>	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open
4	<p>Define a Supply Chain Risk Management strategy to drive the development and implementation of policies and procedures for:</p> <ul style="list-style-type: none"> 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; c. How counterfeit components are prevented from entering the DNFSB supply chain. 	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 2.	Open - DNFSB finalized the <i>Supply Chain Risk Management Strategic Plan</i> , dated August 17, 2022. However, the strategy does not describe in detail how recommendation items a – c are managed.
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.	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open
6	Integrate the Configuration Management Plan with risk management and continuous monitoring programs and utilize lessons learned to make improvements to this plan.	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

Recommendation Number	Recommendation	DNFSB's Status	Auditor's Position on Status
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.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 1.	Open
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 1.	Open
9	Update agency strategic planning documents to include clear milestones for implementing strong authentication, the Federal Identity, Credential and Access Management (ICAM) architecture and OMB M-19-17 <i>Enabling Mission Delivery through Improved Identity, Credential, and Access Management</i> , and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program.	This recommendation remains open. Estimated target completion date: FY 2023.	Open
10	Conduct the agency's annual breach response plan exercise for FY 2021.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 1.	Open
11	Continue efforts to develop and implement role-based privacy training for users with significant privacy or data protection related duties.	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open – DNFSB did not provide the final version of the policy until August 2022, after completion of fieldwork. In addition, management did not provide evidence of how the policy has been implemented.

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

Recommendation Number	Recommendation	DNFSB's Status	Auditor's Position on Status
12	Formally document requirements and procedures for the completion of role-based training and enforcement methods in place for individuals who do not complete role-based training.	This recommendation is closed. DNFSB has formally documented requirements and procedures for the completion of role-based training.	Closed
13	Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open
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.	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open
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 2022 Quarter 4.	Open
16	Defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program.	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open
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.	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open
18	Consistently test the incident response plan annually.	This recommendation remains open. Estimated target completion date: FY 2022 Quarter 4.	Open - In the prior FISMA report, DNFSB management disagreed with this recommendation, and the

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

Recommendation Number	Recommendation	DNFSB's Status	Auditor's Position on Status
			recommendation remains unresolved.
19	Update the Agency's incident response plan to reflect the United States Computer Emergency Readiness Team (US-CERT) incident reporting guidelines.	This recommendation is closed. The <i>Incident Response Plan</i> was updated to reflect US-CERT incident reporting guidelines (e.g., reporting within an hour to US-CERT).	Closed
20	Allocate and train staff with significant incident response responsibilities.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 1.	Open
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.	This recommendation remains open. Estimated target completion date: FY 2023 Quarter 2.	Open
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
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 1.	Open
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 1.	Open

**Defense Nuclear Facilities Safety Board
FY 2022 Audit of the DNFSB's Implementation of the FISMA**

APPENDIX IV: DNFSB's MANAGEMENT COMMENTS

An exit briefing was held with the agency on September 23, 2022. Prior to this meeting, DNFSB management reviewed a discussion draft and provided comments that have been incorporated into this report as appropriate. As a result, DNFSB 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.