MEMORANDUM

DATE: September 30, 2024

TO: Mary J. Buhler
Executive Director of Operations

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

SUBJECT: AUDIT OF THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2024 (DNFSB-24-A-05)

The Office of the Inspector General (OIG) contracted with Sikich to conduct the *Audit of the Defense Nuclear Facilities Safety Board's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024*. Attached is Sikich's final report on the audit. The objective was to assess the effectiveness of the information security policies, procedures, and practices of the Defense Nuclear Facilities Safety Board (DNFSB). The findings and conclusions presented in this report are the responsibility of Sikich. The OIG's responsibility is to provide oversight of the contractor's work in accordance with generally accepted government auditing standards.

The report presents the results of the subject audit. Following the exit conference, the agency's staff indicated that they had no formal comments for inclusion in this report.

Based on its assessment of the period October 1, 2023, through June 30, 2024, Sikich found that the DNFSB has not established an effective agency-wide information security program or effective information security practices. There are weaknesses that impact the agency's ability to adequately protect the DNFSB's systems and information.

Please provide information on actions taken or planned on each of the recommendations within 30 calendar days of the date of this report. Actions taken or planned are subject to OIG follow-up.

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 Mike Blair, Team Leader, at 301.415.8399.

Attachment:
As stated

cc: J. Biggins, GM
T. Reddish, DGM
T. Tadlock, OEDO
G. Garvin, OEDO

SIKICH®

Performance Audit of the Defense Nuclear Facilities Safety Board's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024

Submitted to the
Office of the Inspector General for the
Defense Nuclear Facilities Safety Board

Performance Audit Report

September 30, 2024

ACCOUNTING TECHNOLOGY ADVISORY

SIKICH®

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

SIKICH.COM

September 30, 2024

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

Dear Mr. Feitel:

Sikich CPA LLC (Sikich)[1] is pleased to submit the attached report detailing the results of our performance audit of the Defense Nuclear Facilities Safety Board's (DNFSB's) information security program and practices for fiscal year 2024 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires federal agencies, including the DNFSB, to perform an annual independent evaluation of their information security program and practices. FISMA states that the evaluation is to be performed by the agency's Inspector General (IG) or by an independent external auditor as determined by the IG. The Office of the Inspector General for the DNFSB engaged Sikich to conduct this performance audit.

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

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We describe our objective, scope, and methodology in **Appendix B: Objective, Scope, and Methodology**.

We appreciate the assistance provided by DNFSB management and staff.

Sincerely,

Sikich CPA LLC

September 30, 2024

[1] Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's (CLA's) federal practice, including its work for the Defense Nuclear Facilities Safety Board.

TABLE OF CONTENTS

I. Executive Summary

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also requires agency Inspectors General (IGs) to assess the effectiveness of their agency's information security program and practices. The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

The Office of the Inspector General (OIG) for the Defense Nuclear Facilities Safety Board (DNFSB) engaged Sikich CPA LLC (Sikich)[2] 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 DNFSB's information security policies, procedures, and practices.

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

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

For this audit, we reviewed selected controls outlined in NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the FY 2024 IG FISMA reporting metrics, for the DNFSB general support system (GSS). The audit covered the period from October 1, 2023, through June 30, 2024. We performed audit fieldwork from January to June 2024.

[2] Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's (CLA's) federal practice, including its work for the Defense Nuclear Facilities Safety Board.

[3] See OMB M-24-04 online here.

[4] See the Fiscal Year (FY) 2023 – 2024 IG FISMA Reporting Metrics online here. We submitted our responses to the FY 2024 IG FISMA Reporting Metrics to the DNFSB OIG as a separate deliverable under the contract for this audit.

[5] Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.

[6] Supplemental metrics are assessed at least once every two years; they represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

II. Summary of Results

We concluded the DNFSB has not implemented effective information security policies, procedures, and practices. Specifically, the DNFSB achieved an overall maturity level of Level 3: *Consistently Implemented*. To be considered effective, the DNFSB's information security program must be rated Level 4: *Managed and Measurable.* **Table 1** below summarizes the overall maturity levels for each security function and domain in the Fiscal Year (FY) 2024 IG FISMA Reporting Metrics.

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

Cybersecurity Framework Security Functions	Maturity Level by Function	Domain	Maturity Level by Domain
Identify	Level 3: *Consistently Implemented*	Risk Management	Level 3: *Consistently Implemented* (Not Effective)
		Supply Chain Risk Management	Level 1: *Ad-Hoc* (Not Effective)
Protect	Level 4: *Managed and Measurable*	Configuration Management	Level 4: *Managed and Measurable* (Effective)
		Identity and Access Management	Level 4: *Managed and Measurable* (Effective)
		Data Protection and Privacy	Level 3: *Consistently Implemented* (Not Effective)
		Security Training	Level 4: *Managed and Measurable* (Effective)
Detect	Level 3: *Consistently Implemented*	Information Security Continuous Monitoring	Level 3: *Consistently Implemented* (Not Effective)
Respond	Level 2: *Defined*	Incident Response	Level 2: *Defined* (Not Effective)
Recover	Level 3: *Consistently Implemented*	Contingency Planning	Level 3: *Consistently Implemented* (Not Effective)
Overall	**Level 3: *Consistently Implemented* (Not Effective)**		

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

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

- Continued implementing its Continuous Diagnostics and Mitigation (CDM) program to obtain additional tools and dashboards to monitor its security posture.
- Conducted an independent security control assessment for its GSS.
- Ensured multi-factor authentication was in place for its network.
- Established performance metrics for information system contingency plan tests.

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

- The DNFSB did not fully implement its vulnerability management program (Finding 1: Protect Function – Configuration Management Domain).
- The DNFSB should improve its privacy training program (Finding 2: Protect Function – Data Protection and Privacy Domain).

- The DNFSB should update its incident response plans to reflect lessons learned and ensure key personnel participate in incident response exercises (Finding 3: Respond Function – Incident Response Domain).

In addition, the DNFSB has outstanding prior-year recommendations that significantly impact the IG FISMA Reporting Metrics. Specifically, at the beginning of FY 2024, the DNFSB had 36 open recommendations from prior FISMA audits dating from 2019 through 2023. During our FY 2024 audit, we found that the DNFSB took corrective actions to address 22 recommendations, and we consider those recommendations closed. Corrective actions are in progress for the 14 recommendations that remain open.

To fully progress toward a "Managed and Measurable" maturity level, 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, Incident Response, and Contingency Planning domains of the IG FISMA Reporting Metrics. Additionally, to demonstrate measurable improvement in establishing an effective information security program, the DNFSB must focus on remediating prior-year recommendations in a timely manner and prioritizing those recommendations related to the core metrics. Implementing these recommendations will help the DNFSB mature its information security program and improve its effectiveness.

In addition, the DNFSB could consider developing a strategy that includes resource commitments to continue addressing corrective actions necessary to show steady, measurable improvement in its information security program. Developing such a strategy may require the DNFSB to allocate sufficient resources, including staffing, to continue remediating audit recommendations in a timely manner.

As a result of the weaknesses noted, we made four new recommendations to assist the DNFSB in strengthening its information program. Additionally, we noted that 14 prior-year recommendations remain open.[7]

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

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

III. Audit Results

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

Security Function: Identify

The objective of the Identify function is to develop an organizational understanding of the business context and the resources that support functions that are critical for managing cybersecurity risk to systems, people, assets, data, and capabilities. We determined that the maturity level of the DNFSB's Identify function is Level 3: *Consistently Implemented*.

Risk Management

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

We determined that the maturity level of the DNFSB's Risk Management domain is Level 3: *Consistently Implemented*. The DNFSB has advanced its risk management program by improving its system inventory processes through the use of automated tools, categorizing information systems, continuing the implementation of its CDM program, and performing a security control assessment for the DNFSB GSS.

However, we noted that the DNFSB has four open prior-year recommendations in the Risk Management domain that relate to documenting an information security architecture, implementing an enterprise risk management program, and implementing a centralized view of risk across the organization.[8]

Supply Chain Risk Management

An agency with an effective supply chain risk management program (1) ensures that external providers' products, system components, systems, and services are consistent with the agency's cybersecurity and supply chain risk management requirements, and (2) reports qualitative and quantitative performance measures on the effectiveness of its supply chain risk management program.

We determined that the maturity level of the DNFSB's Supply Chain Risk Management domain is Level 1*: Ad-Hoc*. We noted that four prior-year recommendations from previous FISMA reports remain open; further, the DNFSB's *Supply Chain Risk Management Strategic Plan* and *Supply Chain Risk Management Operating Procedures* remained in draft form, and the DNFSB has not finalized and implemented these documents.[9]

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

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

Security Function: Protect

The objective of the Protect function is to develop and implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event. We determined that the maturity level of the DNFSB's Protect function is Level 4: *Managed and Measurable*.

Configuration Management

An agency with an effective configuration management program employs automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; consistently implements its configuration management policies, procedures, plans, and strategy at all levels of the organization; centrally manages its flaw remediation process; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its configuration management program.
We determined that the maturity level of the DNFSB's Configuration Management domain is Level 4: *Managed and Measurable.* The DNFSB demonstrated strengths in this area by maintaining configuration management plans and policies and procedures, establishing configuration baselines, and monitoring its systems for baseline compliance.

However, we identified areas for improvement in the DNFSB's vulnerability management program and noted that the DNFSB has one open prior-year recommendation in the Configuration Management domain[10] related to establishing a requirement for improving the change control process through remedial training.

Finding 1: The DNFSB Did Not Fully Implement Its Vulnerability Management Program.

Based on our review of the DNFSB's vulnerability management dashboard, generated on February 14, 2024, and its vulnerability-related plans of action and milestones (POA&Ms), we found the following:

- The DNFSB has not remediated vulnerabilities in a timely manner, in accordance with its *Vulnerability Management Operating Procedure*. Specifically, we noted that as of February 14, 2024, the DNFSB's vulnerability management dashboard reported 381 vulnerabilities aged between 31 and 60 days, 42 vulnerabilities aged between 61 and 90 days, 178 vulnerabilities aged between 91 and 180 days, and 833 vulnerabilities aged more than 180 days.
- The DNFSB has not fully implemented a risk management program to prioritize and address vulnerabilities. Specifically, the DNFSB did not incorporate risk-based, prioritized decision-making when developing vulnerability-based POA&Ms in accordance with its *Vulnerability Management Operating Procedure*.

The DNFSB Chief Information Security Officer (CISO) stated that DNFSB management was aware of the prior-year finding relating to vulnerability management and was in the process of remediating this finding. Specifically, DNFSB management updated the *Vulnerability Management Operating Procedure*, dated February 21, 2023, to provide details on vulnerability remediation timelines; the process of opening POA&Ms, as applicable; and the use of risk-based decision-making, as applicable.

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

Although the DNFSB has revised its policies and procedures relating to vulnerability management, it is still in the process of implementing the revised policies and procedures. The revised policies and procedures called for implementing a risk-based process for prioritizing vulnerabilities and opening POA&Ms, and for making risk-based decisions when the DNFSB was unable to address vulnerabilities in a timely manner.

The DNFSB's *Vulnerability Management Operating Procedure*, dated February 21, 2023, states:

> *D. Vulnerability Prioritization:*
>
> *In accordance with Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities (KEV), the DNFSB shall prioritize the remediation of all vulnerabilities that CISA labels as KEVs. As a result, KEVs shall be remediated within 14 days.*
>
> *For all other vulnerabilities, the DNFSB shall use the Common Vulnerability Scoring System (CVSS) criticality ratings to prioritize remediation and mitigation efforts. Non-KEV Critical and High vulnerabilities shall be remediated within 30 days. Medium and Low vulnerabilities shall be remediated within 90 days.*
>
> *E. Vulnerability Remediation and Mitigation:*
>
> *The DNFSB shall remediate vulnerabilities via patching, configuration changes, or other methods, as appropriate to the specific vulnerability. If a remediation is not available, mitigation shall be attempted to lessen the potential impact of the vulnerability. All vulnerability remediation and mitigation efforts shall follow the DNFSB Configuration Management process. Vulnerabilities that are not able to be remediated shall be documented on a POA&M, listing any necessary mitigations.*
>
> *F. Verification of Remediation and Mitigation:*
>
> *Once remediation has taken place, the Cybersecurity team shall use Qualys to rescan the affected assets to verify the vulnerability is no longer present. If only mitigation is possible, the Cybersecurity team shall verify the appropriate security controls have been enforced and are documented within the POA&M.*

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

Because DNFSB management made progress updating the *Vulnerability Management Standard Operating Procedure,* we have closed the prior year recommendation[11] and issued the following recommendation to focus on the implementation of the procedures:

[11] Recommendation 7, *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).

Recommendation 1: We recommend that the DNFSB implement the DNFSB's Vulnerability Management Standard Operating Procedure for vulnerability and compliance management based on the risk and level of effort involved in mitigating confirmed vulnerabilities on a case-by-case basis, such as:

a) Remediating vulnerabilities in accordance with the DNFSB Vulnerability Management Standard Operating Procedure.

b) Opening plans of action and milestones to track critical and high-risk vulnerabilities that the DNFSB cannot address within 30 days.

c) Preparing risk-based decisions in unusual circumstances in which a technical or cost limitation makes it infeasible to mitigate a critical or high-risk vulnerability, including identifying documented, effective compensating controls coupled with a clear timeframe for planned remediation.

Identity and Access Management

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

We determined that the maturity level of the DNFSB's Identity and Access Management domain is Level 4: *Managed and Measurable.* The DNFSB demonstrated strengths in this area by implementing multi-factor authentication for network access for both non-privileged and privileged users and periodically recertifying privileged user access rights.

However, we found that the DNFSB has opportunities to improve its Identity and Access Management program by implementing the four open prior-year recommendations in this area.[12] These recommendations relate to event logging maturity; continuing efforts to develop the DNFSB's Identity, Credential, and Access Management (ICAM) strategy; and implementation of automated controls for managing user inactivity.

Data Protection and Privacy

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

We determined that the maturity level of the DNFSB's Data Protection and Privacy domain is Level 3: *Consistently Implemented.* The DNFSB demonstrated strengths in this area by protecting data through its life cycle (i.e., at rest, in transit, and through destruction), monitoring in-bound and out-bound traffic, and ensuring that the independent security control assessment includes privacy controls.

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

However, we noted that the DNFSB has two open prior-year recommendations in this area related to performing a breach response exercise and developing role-based privacy training.[13] Additionally, the DNFSB's privacy training program needs improvement, as noted below:

Finding 2: The DNFSB Should Improve Its Privacy Training Program.

We identified the following issues related to the DNFSB's privacy awareness training and privacy role-based training.

Privacy Awareness Training
Based on our inspection of the DNFSB's annual Privacy Act training records, we found that, as of November 7, 2023, 23 of the DNFSB's 143 employees and contractors had not yet attended the annual Privacy Act training. The Director of Operational Services stated that the DNFSB divided its Privacy Act training into two training sessions but did not record attendance for one of the two sessions. As a result, the DNFSB did not maintain full training completion records.

Privacy Role-Based Training
Based on our inspection of the DNFSB's Privacy Act training presentation, we found that the DNFSB was still in the process of developing role-based privacy training for users with significant privacy or data protection-related duties. The Director of Operational Services stated that, although the DNFSB made improvements in developing privacy role-based training (e.g., developing System of Records Notices [SORN] training), more work is needed to develop broader role-based privacy training to cover areas related to personally identifiable information (PII) processing and transparency controls.

NIST Special Publication 800-53, Revision 5 (dated December 10, 2020), *Security Controls Related to Training Programs*, specifies the following:

- *Awareness and Training (AT-2), Literacy Training and Awareness, requires that the agency provide privacy literacy training to system users (including managers, senior executives, and contractors) upon initial hire and on an annual basis thereafter.*
- *AT-3, Role-Based Training, requires agencies to provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities] prior to authorizing access to the system, information, or performing assigned duties, and annual thereafter.*
- *AT-3, Enhancement 5, requires that agencies provide initial and organizational defined training in the employment and operation of PII processing and transparency controls.*

The DNFSB's *Security and Privacy Awareness and Training Program Standard Operating Procedure*, dated August 15, 2023, requires that the DNFSB provide security and privacy literacy training to system users (including managers, senior executives, and contractors) as part of the initial training for new users and annually thereafter.

Lack of privacy awareness training may increase the risk that individuals do not have sufficient knowledge regarding how to identify and respond to a suspected incident that involves PII and sensitive agency information. Additionally, the lack of privacy role-based training may increase the risk that individuals with significant duties related to privacy or data protection may not fully understand their roles and responsibilities in safeguarding PII and sensitive agency information.

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

The FY 2021[14] FISMA evaluation report noted that a recommendation related to privacy role-based training remained open. Because this recommendation still remains open, we are not making any new recommendations related to the role-based training finding. However, we are making the following recommendation to address privacy awareness training.

> ***Recommendation 2:*** We recommend that the DNFSB (1) ensure that personnel complete privacy awareness and literacy training upon initial hire and annually thereafter, and (2) maintain training records in accordance with the *DNFSB Security and Privacy Awareness and Training Program Standard Operating Procedure*.

Security Training

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

We determined that the maturity level for the DNFSB's Security Training domain is Level 4: *Managed and Measurable* and did not identify any findings related to this domain. The DNFSB has shown strengths in this area by conducting a workforce assessment and providing annual security awareness and role-based training to its employees.

Security Function: Detect

The objective of the Detect function is to implement continuous monitoring of control activities to discover and identify cybersecurity events in a timely manner. Cybersecurity events[15] include anomalies and changes in the organization's IT environment that may impact organizational operations, including operating relating to the agency's mission, capabilities, or reputation. We determined that the maturity level of the DNFSB's Detect function is Level 3*: Consistently Implemented.*

Information Security Continuous Monitoring

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

We determined that the maturity level for the DNFSB's Information Security Continuous Monitoring domain is Level 3: *Consistently Implemented.* The DNFSB demonstrated improvements in this area by performing an independent security control assessment for the DNFSB GSS and establishing a process for the CISO to review monthly security reports.

[14] Recommendation 11, *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).
[15] https://csrc.nist.gov/glossary/term/cybersecurity_event

However, we noted that there are two open prior-year recommendations in this area related to establishing performance metrics to manage and optimize all domains of the DNFSB's information security program more effectively.[16]

Security Function: Respond

The objective of the Respond function is to implement processes to contain the impact of detected cybersecurity events. Such processes include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. We determined that the maturity level of the DNFSB's Respond function is Level 2: *Defined*.

Incident Response

An agency with an effective incident response program:

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

We determined that the maturity level of the DNFSB's Incident Response domain is Level 2: *Defined.* The DNFSB has developed incident response policies and procedures. However, it has not updated its incident response plans to address lessons learned from an incident response exercise, and not all key personnel participated in the incident response exercise, as noted below. In addition, the DNFSB has an open recommendation in this area related to implementing requirements across all event logging maturity tiers to ensure the agency logs and tracks events in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.[17]

Finding 3: The DNFSB Should Update Its Incident Response Plans to Reflect Lessons Learned and Ensure Key Personnel Participate in Incident Response Exercises.

We identified the following issues related to the DNFSB's updates to its incident response plans and the participation of key personnel in its incident response exercise.

- ***Incident Response Plan Updates:*** The DNFSB's *Incident Response Plan*, dated December 7, 2023, and its *Incident Response Process Guide Cyber Playbook*, dated September 2022, were still in draft form, and the DNFSB had not updated them to address lessons learned from the incident response tabletop exercise that occurred on May 24, 2023.

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

Specifically, the *DNFSB Tabletop Exercise – Supply Chain and Insider Threat Incident Response*, dated May 24, 2023, recommended that the DNFSB update the *Incident Response Plan* and *Incident Response Process Guide Cyber Playbook* to add or revise sections related to notifications and law enforcement involvement, as well as to add or revise a contact chart and a responsibilities table.

- ***Incident Response Exercise Participation:*** The *DNFSB Tabletop Exercise – Supply Chain and Insider Threat Incident Response*, dated May 24, 2023, did not include all personnel with incident response responsibilities.

The DNFSB CISO stated that, as of May 7, 2024, the *Incident Response Plan* and *Incident Response Process Guide Cyber Playbook* were living documents that were in the process of undergoing management review. The CISO further stated that the May 24, 2023, incident response exercise was limited in scope; therefore, it did not include all members with incident response responsibilities. The CISO noted that the DNFSB is planning a more comprehensive incident response exercise for the June or July 2024 timeframe that would involve all parties responsible for the incident response process. The DNFSB will update the *Incident Response Plan* and *Incident Response Process Guide Cyber Playbook* based on the results of the tabletop exercise.

NIST Special Publication 800-53, Revision 5, *Security Controls Related to Incident Response*, specifies the following:

- Security control IR-8, *Incident Response Plan*, requires that an incident response plan is updated to address changes or problems encountered during testing.
- Security control IR-2, *Incident Response Training*, requires that the organization provides incident response training to users consistent with assigned roles.

Without incorporating lessons learned from incident response exercises into incident response plans, the DNFSB increases the risk that the plans may be outdated and that the DNFSB may not implement necessary changes to the plans. Further, it could increase the risk that the DNFSB may not respond to an actual incident timely or effectively.

In addition, without including all personnel with incident response responsibilities in an incident response exercise, the DNFSB increases the risk that personnel may not be adequately prepared to assume their assigned roles and responsibilities during an actual incident.

> ***Recommendation 3:*** We recommend that the DNFSB update and finalize the *Incident Response Plan* and *Incident Response Process Guide Cyber Playbook* to incorporate lessons learned from incident response exercises.
>
> ***Recommendation 4:*** We recommend that the DNFSB ensure all personnel with incident response responsibilities participate in incident response exercises.

Security Function: Recover

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

We determined that the maturity level of the DNFSB's Recover function is Level 3: *Consistently Implemented*.

Contingency Planning

An agency with an effective contingency planning program establishes contingency plans; employs automated mechanisms to thoroughly and effectively test system contingency plans; communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures regarding the effectiveness of information system contingency planning program activities.

We determined that the maturity level for the DNFSB's Contingency Planning domain is Level 3: *Consistently Implemented.* The DNFSB demonstrated improvement in this area by documenting contingency plans, establishing performance metrics to capture during information system contingency plan tests, and implementing backup and recovery controls.

However, we noted that the DNFSB has two open prior-year recommendations in the Contingency Planning domain[18] related to performing a Business Impact Analysis (BIA) on a timely basis and updating the DNFSB's contingency planning policies and procedures to address Information and Communications Technology (ICT) supply chain risk.

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

APPENDIX A: BACKGROUND

Federal Information Security Modernization Act of 2014

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Agencies must also report annually to the OMB and to Congressional committees on the effectiveness of their information security program and practices. In addition, FISMA requires agency IGs to assess the effectiveness of their agency's information security program and practices.

NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to federal information systems. The standards prescribed include information security standards that provide minimum information security requirements necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with Federal Information Processing Standards issued by NIST. In addition, NIST develops and issues Special Publications as recommendations and guidance documents.

FISMA Reporting Requirements

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

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

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

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

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

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

The foundational levels of the maturity model in the IG FISMA Reporting Metrics focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 3** 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 3: IG Evaluation Maturity Levels

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

Source: FY 2024 IG FISMA Reporting Metrics

APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

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

Scope

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The scope of this performance audit covered the DNFSB's information security program and practices consistent with FISMA and reporting instructions that the OMB and the DHS issued for FY 2024. The scope also included assessing selected controls from NIST Special Publication 800-53, Revision 5, to support the FY 2024 IG FISMA Reporting Metrics for the DNFSB GSS.

Table 4: Description of System Selected for Testing

System Name	Description
DNFSB GSS	The DNFSB GSS is an Ethernet-based network that connects all user workstations with centralized file servers used to store data and host applications. Information processed consists of staff work products and administrative information. Information is generally created on user workstations and saved to the file servers.

Source: DNFSB GSS System Security Plan

The audit also included an evaluation of whether the DNFSB took corrective actions to address open recommendations from the FY 2023 FISMA audit,[19] FY 2022 FISMA audit,[20] FY 2021 FISMA evaluation,[21] FY 2020 FISMA evaluation,[22] and FY 2019 FISMA evaluation.[23]

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

Methodology

To accomplish our objective, we completed the following procedures:

- Evaluated key components of the DNFSB's information security program and practices, consistent with FISMA and reporting instructions that the OMB and the DHS issued for FY 2024.

[19] *Audit of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023* (Report No. DNFSB-23-A-04, issued September 29, 2023).
[20] *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).
[21] *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).
[22] *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).
[23] *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).

- Focused our testing activities on assessing the maturity of the 20 core and 17 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Inquired of DNFSB management and staff.
- Considered guidance contained in OMB's Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, when planning and conducting our work.
- Evaluated select security processes and controls at the program level, as well as for a non-statistical sample of one internally maintained DNFSB information system from the 33 systems in the DNFSB's system inventory. The DNFSB's GSS is the only agency-owned system. The remainder are either third-party shared services or cloud services. Due to the size and complexity of the DNFSB, we selected the agency-owned GSS for testing. The GSS is a moderate-impact system, based on NIST Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information System*.
- Analyzed the DNFSB GSS, including reviewing selected system documentation and other relevant information, as well as testing selected security controls to support the IG FISMA Reporting Metrics.
- Reviewed the status of prior-year FISMA recommendations. See **Appendix C** for the status of the prior-year recommendations.

The FY 2023 IG FISMA Reporting Metrics introduced a calculated average scoring model that was continued for the FY 2024 FISMA audit. As part of this approach, IGs must average the ratings for core and supplemental IG FISMA Reporting Metrics independently to determine a domain's maturity level and provide data points for the assessed effectiveness of the program and function. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, calculated averages were not automatically rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, the OMB strongly encouraged IGs to focus on the results of the core IG FISMA Reporting Metrics, as these tie directly to administration priorities and other high-risk areas. The OMB recommended that IGs use the calculated averages of the supplemental IG FISMA Reporting Metrics as a data point to support their risk-based determination of the overall effectiveness of the program and function.

We used the FY 2024 IG FISMA Reporting Metrics guidance[24] to form our conclusions for each Cybersecurity Framework domain and function, as well as for the overall agency rating. Specifically, we focused on the calculated average scores of the core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average scores of the supplemental IG FISMA Reporting Metrics and progress that the DNFSB has made in addressing outstanding prior-year recommendations, to form our risk-based conclusion.

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

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

APPENDIX C: STATUS OF PRIOR-YEAR RECOMMENDATIONS

The table below summarizes the status of the open prior-year recommendations from the FY 2023 FISMA audit, FY 2022 FISMA audit, FY 2021 FISMA evaluation, FY 2020 FISMA evaluation, and FY 2019 FISMA evaluation.[25] At the time of testing and IG FISMA Reporting Metric submission, 14 of the 36 prior-year recommendations from the audits and evaluations referenced above remained open.

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

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
DNFSB-23-A-04 **FY 2023 FISMA Audit** **Recommendation 1**	We recommend that DNFSB's Chief Information Security Officer acquires resources to adequately support the procurement, onboarding, and implementation of requirements across all event logging maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).	This recommendation remains open. Estimated target completion date: FY 2025 Quarter (Q) 2 DNFSB management indicated that they will ensure the DNFSB captures and stores all criticality level 2 and 3 logs in Log Analytics Workspace by FY 2025 Q2.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Identity Access Management** **Incident Response**
DNFSB-22-A-07 **FY 2022 FISMA Audit** **Recommendation 1**	Implement a process to ensure a security control assessment for the DNFSB GSS is completed and documented on an annual basis.	An independent party performed a security control assessment of the DNFSB GSS in June 2023.	Closed We inspected the June 2023 security control assessment and noted that an independent party performed a security control assessment for the DNFSB GSS.	**Risk Management** **Information Security Continuous Monitoring**
DNFSB-22-A-07 **FY 2022 FISMA Audit**	Implement a process to validate the DNFSB GSS security authorization is	The DNFSB completed an external security assessment in	Closed	**Information Security**

[25] See footnotes 18, 19, 20, 21, and 22.

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 2	maintained in accordance with DNFSB policy.	June 2023 and issued an updated Authority to Operate (ATO) for the DNFSB GSS in July 2023. This recommendation is closed.	The OIG reviewed the documentation supporting the June 2023 external security assessment and the July 2023 ATO and determined that the DNFSB is maintaining the security authorization in accordance with DNFSB policy.	**Continuous Monitoring**
DNFSB-22-A-07 **FY 2022 FISMA Audit** **Recommendation 5**	Complete the implementation of the configuration management training program and provide periodic refreshers to ensure evidence requirements are captured for change tickets.	The DNFSB considers this recommendation to be fully remediated and requests closure of this recommendation.	Closed The OIG noted an improvement in change documentation for the sampled changes during the FISMA audit. The DNFSB provided documentation supporting its implementation of the configuration management training program, as well as documentation supporting that it provides periodic refreshers to ensure it captures evidence requirements for change tickets.	**Configuration Management**
DNFSB-22-A-07 **FY 2022 FISMA Audit** **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 Binding Operational Directive (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	The DNFSB has revised its *Vulnerability Management Operating Procedure* to include prioritizing mitigation, creating POA&Ms for vulnerabilities that it cannot remediate within 30 days, and making risk-based decisions regarding vulnerabilities. The DNFSB requests closure of this recommendation.	Closed We inspected the DNFSB's *Vulnerability Management Operating Procedure* and noted that the procedures included prioritizing mitigation, creating POA&Ms for vulnerabilities that it cannot remediate within 30 days, and making risk-based decisions regarding vulnerabilities.	**Configuration Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	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-22-A-04 FY 2021 FISMA Evaluation **Recommendation 1**	Update the ISA and use it 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 2025. The DNFSB is currently drafting an Information Security Architecture (ISA) as part of the Federal Enterprise Architecture documentation.	Closed We noted this recommendation was a duplicate of Recommendation 2 in DNFSB-21-A-04 (FY 2020 FISMA Evaluation); therefore, we have closed this recommendation.	**Risk Management**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 2**	Using the results of recommendation one above: a. Utilizing guidance from the NIST Special Publication 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 POA&Ms to remediate vulnerabilities.	This recommendation remains open. The DNFSB is collaborating to determine appropriate performance metrics, with an estimated completion date of FY 2025.	Closed We noted this recommendation was a duplicate of Recommendations 3b, 3c, and 3d in DNFSB-21-A-04 (FY 2020 FISMA Evaluation); therefore, we have closed this recommendation.	**Risk Management** **Information Security Continuous Monitoring**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 3**	Update the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, to include:	The DNFSB requests closure of this recommendation.	Closed The DNFSB has updated its Risk Management Framework and Risk Assessment Policy to document the current roles, responsibilities,	**Risk Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	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.		policies, and procedures of the DNFSB environment.	
DNFSB-22-A-04 FY 2021 FISMA Evaluation **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.	This recommendation remains open. Estimated target completion date: FY 2024 Q4 The DNFSB has drafted a *Supply Chain Risk Management Strategic Plan* and *Supply Chain Risk Management Operating Procedures*. These documents remain under review.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Supply Chain Risk Management**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **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*.	The DNFSB requested closure of this recommendation.	Closed The OIG noted an improvement in change documentation for the sampled changes during the FISMA audit. The OIG verified that the DNFSB conducted remedial training to re-enforce requirements for documenting the 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*.	**Configuration Management**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **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,	This recommendation remains open. Estimated target completion date: FY 2024 Q4	Closed We noted this recommendation was a duplicate of Recommendation 9 in DNFSB-21-A-04 (FY 2020 FISMA Evaluation);	**Identity and Access Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	emergency, and inactive accounts, as appropriate.	The DNFSB is currently establishing an enterprise risk management program. Once established, the program will review this recommendation.	therefore, we have closed this recommendation.	
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 8**	Continue efforts to implement data loss prevention functionality for the Microsoft Office 365 environment.	The DNFSB requested closure of this recommendation.	Closed The DNFSB has implemented data loss prevention functionality for the Microsoft Office 365 environment through the Microsoft Sentinel and Purview products.	**Data Protection and Privacy**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 9**	Update agency strategic planning documents to include clear milestones for implementing strong authentication, the Federal ICAM architecture and OMB Memorandum (M)-19-17, and phase 2 of DHS's CDM program.	This recommendation remains open. Estimated target completion date: FY 2024 Q4. The DNFSB has drafted an *Identification and Authentication Operating Procedures* document. This document is currently under review.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Identity and Access Management**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 10**	Conduct the agency's annual breach response plan exercise for FY 2021.	This recommendation remains open. The DNFSB has scheduled a breach response tabletop exercise for Q3 FY 2024.	Closed We noted this recommendation was a duplicate of Recommendation 11 in DNFSB-21-A-04 (FY 2020 FISMA Evaluation); therefore, we have closed this recommendation.	**Data Protection and Privacy**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 11**	Continue efforts to develop and implement role-based privacy training for users with significant privacy or data protection related duties.	The DNFSB requested closure of this recommendation.	Open Based on our testing, we noted that the DNFSB is currently in the process of developing role-based privacy training. Refer to Finding #2 above.	**Data Protection and Privacy**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 13**	Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.	The DNFSB requested closure of this recommendation.	Closed The OIG noted that the DNFSB has made progress in refining procedures such as the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* to support adoption of an ongoing authorization model. The OIG verified that the DNFSB had implemented the updated monitoring and assessment procedures and performed the system authorization.	**Information Security Continuous Monitoring**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 20**	Allocate and train staff with significant incident response responsibilities.	The DNFSB requested closure of this recommendation.	Closed The DNFSB has provided training to staff that have significant incident response responsibilities.	**Incident Response**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 22**	Develop and track metrics related to the performance of contingency planning and recovery related activities.	The DNFSB requested closure of this recommendation.	Closed The DNFSB has established performance metrics captured through the information system contingency plan test exercises, such as capturing recovery time.	**Contingency Planning**
DNFSB-22-A-04 FY 2021 FISMA Evaluation **Recommendation 23**	Conduct a BIA 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 2024 Q3 The DNFSB is currently establishing an enterprise risk management program. Once established, this program will conduct a BIA.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Contingency Planning**
DNFSB-22-A-04 FY 2021 FISMA Evaluation	Implement role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.	The DNFSB requested closure of this recommendation.	Closed The DNFSB has provided training to staff that have significant	**Contingency Planning**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 24			responsibilities related to contingency planning and disaster recovery.	
DNFSB-21-A-04 FY 2020 FISMA Evaluation **Recommendation 1**	Define an ISA in accordance with the *Federal Enterprise Architecture Framework*.	This recommendation remains open. Estimated target completion date: FY 2024 Q4. The DNFSB is currently drafting an ISA that will meet the standards of the *Federal Enterprise Architecture Framework*.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Risk Management**
DNFSB-21-A-04 FY 2020 FISMA Evaluation **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 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.	This recommendation remains open. Estimated target completion date: FY 2025. The DNFSB is currently drafting an ISA that will meet the standards of the *Federal Enterprise Architecture Framework.*	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Risk Management**
DNFSB-21-A-04 FY 2020 FISMA Evaluation **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	This recommendation remains open. Estimated target completion date: FY 2025.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Risk Management** **Supply Chain Risk Management** **Information Security**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	services being monitored by IT Operations; b. Utilize guidance from the NIST Special Publication 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&Ms to remediate vulnerabilities.	The DNFSB is collaborating to determine appropriate performance metrics. The DNFSB is currently implementing an enterprise risk management program. This program will centrally assess risk for the organization.		**Continuous Monitoring**
DNFSB-21-A-04 FY 2020 FISMA Evaluation **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 the Track-It!, ForeScout, and KACE solutions.	The DNFSB requested closure of this recommendation.	Closed The DNFSB has established a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to its network using a combination of the Microsoft Defender Suite (Endpoint, Identity), Microsoft Intune Endpoint Management, Microsoft Entra Conditional Access, and Qualys vulnerability/ compliance scanning.	**Risk Management**
DNFSB-21-A-04 FY 2020 FISMA Evaluation **Recommendation 5**	Conduct remedial training 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 Management Plan*.	The DNFSB requested closure of this recommendation.	Closed The OIG noted an improvement in change documentation for the sampled changes during the FISMA audit. The OIG verified that the DNFSB conducted remedial training to re-enforce requirements for documenting CCB's approvals and security impact assessments	**Configuration Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
			for changes to the DNFSB's system in accordance with its *Configuration Management Plan*.	
DNFSB-21-A-04 FY 2020 FISMA Evaluation **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 is signed and uploaded to a centralized tracking system.	The DNFSB requested closure of this recommendation.	Closed The DNFSB does not require that new employees and contractors sign a non-disclosure agreement prior to accessing the DNFSB's information systems. Before granting users access to its systems, the DNFSB follows its *New Hire Procedures* document. If the DNFSB creates a user account prior to the user's start date, the DNFSB disables the account until it completes the new hire procedures.	**Identity and Access Management**
DNFSB-21-A-04 FY 2020 FISMA Evaluation **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.	This recommendation remains open. Estimated target completion date: FY 2024 Q4. The DNFSB is currently establishing an enterprise risk management program. Once established, this program will review the risk related to this recommendation.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Identity and Access Management**
DNFSB-21-A-04 FY 2020 FISMA Evaluation **Recommendation 10**	Continue efforts to develop and implement role-based privacy training.	The DNFSB requested closure of this recommendation.	Closed We noted this recommendation was a duplicate of Recommendation 11 in DNFSB-22-A-04 (FY 2021 FISMA Evaluation); therefore, we have closed this recommendation.	**Data Protection and Privacy**
DNFSB-21-A-04 FY 2020 FISMA Evaluation	Conduct the agency's annual breach response plan exercise for FY 2021.	This recommendation remains open.	Open	**Data Protection and Privacy**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
Recommendation 11		Estimated target completion date: FY 2024 Q3. The DNFSB has scheduled a breach response tabletop exercise for Q3 FY 2024.	We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	
DNFSB-21-A-04 FY 2020 FISMA Evaluation **Recommendation 12**	Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.	The DNFSB requested closure of this recommendation.	Closed The OIG noted that the DNFSB has made progress in refining procedures such as the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* to support adoption of an ongoing authorization model. The OIG verified that the DNFSB implemented the monitoring and assessment procedures and updated the system authorization.	**Information Security Continuous Monitoring**
DNFSB-21-A-04 FY 2020 FISMA Evaluation **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: FY 2024 Q4. The DNFSB has drafted a *Supply Chain Risk Management Strategic Plan* and *Supply Chain Risk Management Operating Procedures*. These documents are currently under review.	Closed We noted this recommendation was a duplicate of Recommendation 11 in DNFSB-20-A-05 (FY 2019 FISMA Evaluation); therefore, we have closed this recommendation.	**Supply Chain Risk Management** **Contingency Planning**
DNFSB-20-A-05 FY 2019 FISMA Evaluation **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 for all its GSS components; Cybersecurity Team exports	Recommendation 3a: Closed. Recommendations 3b-3d: Open Estimated target completion date: FY 2025. The DNFSB is collaborating to determine appropriate	Open (Partial Repeat) We noted that the DNFSB partially addressed this recommendation. Recommendation 3a was closed; however, recommendations 3b-3d remain open, as noted below. Recommendation 3a: Closed	**Supply Chain Risk Management** **Information Security Continuous Monitoring** **Risk Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	metrics and vulnerability reports and sends them to the Chief Information Security Officer (CISO) and 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.	performance metrics. In addition, the DNFSB is currently implementing an enterprise risk management program. This program will centrally assess risk for the organization.	Based on our testing, we noted that the DNFSB has established an automated solution for a complete, accurate, and readily available agency-wide view of security configurations for GSS components. This dashboard can be found within Qualys. The Cybersecurity Team is exporting metrics and vulnerability reports to the CIO and CISO for review at least monthly. Recommendations 3b-3d: Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	
DNFSB-20-A-05 FY 2019 FISMA Evaluation **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.	This recommendation remains open. Estimated target completion date: FY 2024 Q4. The DNFSB has revised its *Configuration Management Plan* to include a requirement for remedial training and consequences for failure to follow the appropriate processes. This document is currently under review.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Configuration Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
DNFSB-20-A-05 FY 2019 FISMA Evaluation **Recommendation 8**	Continue efforts to meet milestones of the DNFSB ICAM Strategy necessary for fully transitioning to DNFSB's "to-be" ICAM architecture.	This recommendation remains open. Estimated target completion date: FY 2024 Q4. The DNFSB has drafted an *Identification and Authentication Operating Procedures* document. This document is currently under review.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Identify and Access Management**
DNFSB-20-A-05 FY 2019 FISMA Evaluation **Recommendation 9**	Complete current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.	The DNFSB requested closure of this recommendation.	Closed The OIG noted that the DNFSB has made progress in refining procedures such as the *DNFSB GSS Continuous Monitoring Policies and Procedures Guide* to support adoption of an ongoing authorization model. The OIG reviewed the documentation supporting the external security assessment performed in June 2023 and the updated ATO for the DNFSB GSS performed in July 2023.	**Information Security Continuous Monitoring**
DNFSB-20-A-05 FY 2019 FISMA Evaluation **Recommendation 11**	Based on the results of the 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.	This recommendation remains open. Estimated target completion date: FY 2024 Q4. The DNFSB has drafted a *Supply Chain Risk Management Strategic Plan* and *Supply Chain Risk Management Operating Procedures*. These documents remain under review.	Open We inspected the documentation provided in response to our follow-up questions regarding open prior-year recommendations and determined that corrective action is ongoing.	**Supply Chain Risk Management** **Contingency Planning**

APPENDIX D: MANAGEMENT RESPONSE

DNFSB management reviewed a discussion draft of this report. On September 17, 2024, DNFSB management concurred with the findings and recommendations of this report and chose not to provide formal comments for inclusion in this report.