MEMORANDUM

DATE: September 25, 2025

TO: Mary J. Buhler
Executive Director of Operations

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

SUBJECT: PERFORMANCE AUDIT OF THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2025 (OIG-DNFSB-25-A-05)

The Office of the Inspector General (OIG) contracted with Sikich CPA LLC (Sikich) to conduct the *Performance Audit of the Defense Nuclear Facilities Safety Board's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025*. 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 Sikich's responsibility. The OIG's responsibility was to oversee the contractor's work in accordance with generally accepted government auditing standards.

Based on its assessment for the period of October 1, 2024, through June 30, 2025, Sikich found that the DNFSB has not established an effective agency-wide information security program and practices. There are weaknesses that impact the agency's ability to protect the DNFSB's systems and information adequately.

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.

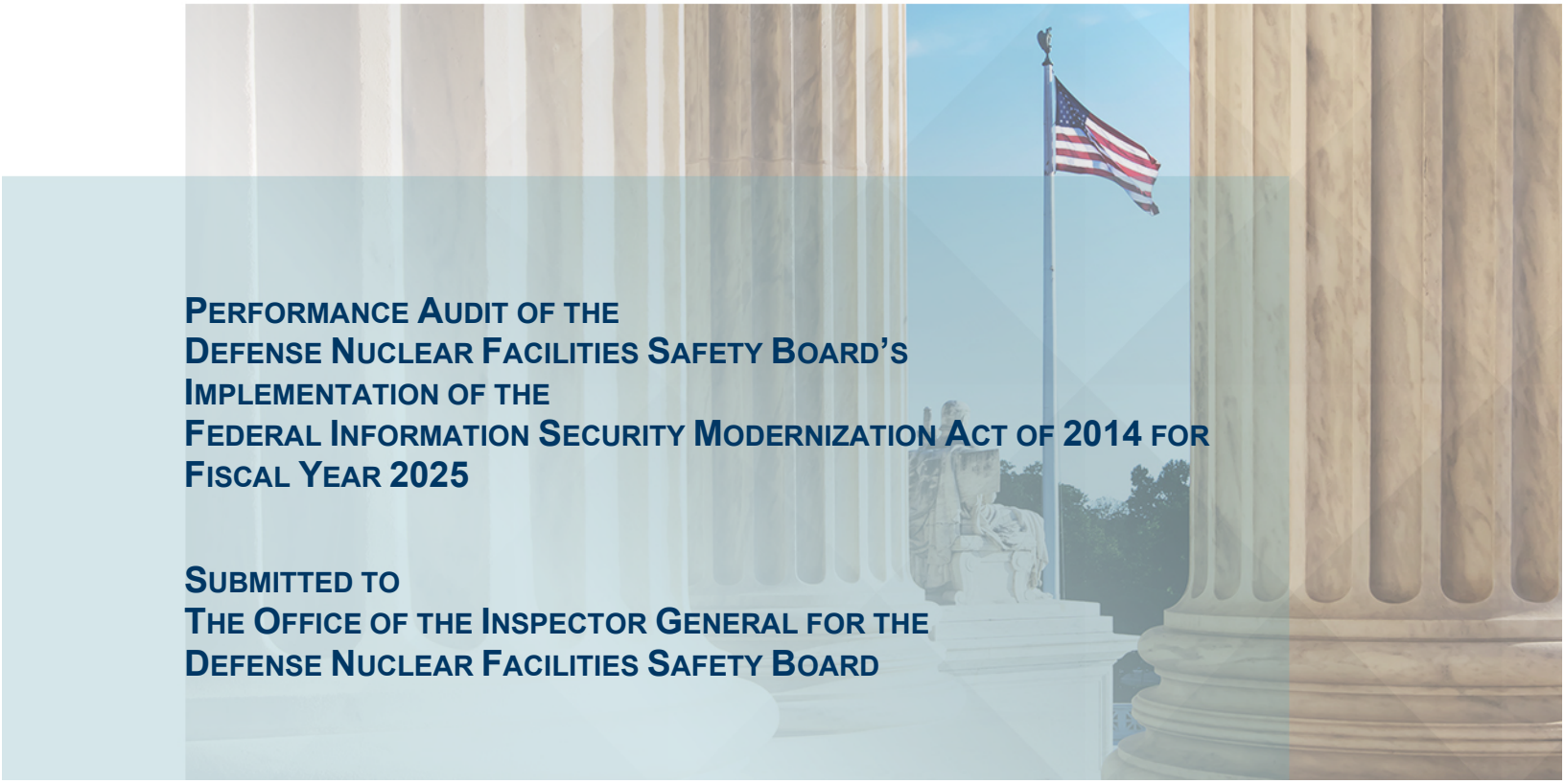
We appreciate the cooperation extended to us by members of your staff during the audit.

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: K. Herrera, DEDO
J. Biggins, DEDRS
G. Garvin, DEDRS

SIKICH®



PERFORMANCE AUDIT OF THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2025

SUBMITTED TO
THE OFFICE OF THE INSPECTOR GENERAL FOR THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD

PERFORMANCE AUDIT REPORT

SEPTEMBER 25, 2025

SIKICH®

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

SIKICH.COM

September 25, 2025

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) is pleased to submit the attached report detailing the results of our performance audit of the Defense Nuclear Facilities Safety Board's (DNFSB) information security program and practices for Fiscal Year (FY) 2025 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, 2024, through June 30, 2025. We performed the work from January through June 2025.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States. 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. 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

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) 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 January 15, 2025, the OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*.[1] This memorandum provides reporting guidance for Fiscal Year (FY) 2025 in accordance with FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. The OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders collaborated to develop the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (FY 2025 IG FISMA Reporting Metrics).[2]

The FY 2025 IG FISMA Reporting Metrics require us to assess the maturity of six function areas in the agency's information security program and practices. For this year's review, the FY 2025 IG FISMA Reporting Metrics required IGs to assess 20 core[3] and 5 supplemental[4] IG FISMA Reporting Metrics across 6 function areas—Govern,[5] 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* or higher. See **Appendix A** for background information on the FISMA reporting requirements.

[1] See OMB M-25-04 online here.
[2] See the FY 2025 IG FISMA Reporting Metrics online here.
[3] Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine the effectiveness of a security program. The core metrics can be found in the FY 2025 IG FISMA Reporting Metrics online here.
[4] Supplemental metrics are assessed at least once every 2 years; they represent important activities conducted by security programs and contribute to the overall evaluation and determination of the effectiveness of the security program. The supplemental metrics can be found in the FY 2025 IG FISMA Reporting Metrics online here.
[5] In February 2024, NIST published the *NIST Cybersecurity Framework (CSF) 2.0*, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an entity's enterprise risk management strategy. As such, the FY 2025 IG FISMA Reporting Metrics added a new IG FISMA function (Govern) that includes a new domain (Cybersecurity Governance) to align with CSF 2.0.

For this audit, Sikich reviewed selected controls from NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the FY 2025 IG FISMA Reporting Metrics, for the DNFSB general support system (GSS). The audit covered the period from October 1, 2024, through June 30, 2025. We performed the audit fieldwork from January to June 2025.

We concluded that the DNFSB has not implemented effective information security policies, procedures, and practices. Specifically, the DNFSB achieved an overall maturity of Level 3: *Consistently Implemented*. **Table 1** below summarizes the overall maturity levels for each Cybersecurity Framework (CSF) function and domain in the FY 2025 IG FISMA Reporting Metrics. We determined that one CSF function achieved a Level 5: *Optimized* maturity level, four CSF functions achieved a Level 3: *Consistently Implemented* maturity level, and one CSF function achieved a Level 2: *Defined* maturity level. To be considered effective, the DNFSB's information security program must be rated at least Level 4: *Managed and Measurable.*

Table 1: Maturity Levels for FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Functions[6]	Maturity Level by Function	Domain	Maturity Level by Domain
Govern	Level 2: *Defined*	Cybersecurity Governance	Level 2: *Defined*
		Cybersecurity Supply Chain Risk Management	Level 2: *Defined*
Identify	Level 3: *Consistently Implemented*	Risk and Asset Management	Level 3: *Consistently Implemented*
Protect	Level 3: *Consistently Implemented*	Configuration Management	Level 2: *Defined*
		Identity and Access Management	Level 4: *Managed and Measurable*
		Data Protection and Privacy	Level 3: *Consistently Implemented*
		Security Training	Level 3: *Consistently Implemented*
Detect	Level 3: *Consistently Implemented*	Information Security Continuous Monitoring	Level 3: *Consistently Implemented*
Respond	Level 5: *Optimized*	Incident Response	Level 5: *Optimized*
Recover	Level 3: *Consistently Implemented*	Contingency Planning	Level 3: *Consistently Implemented*
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 2025 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:

- Updated its *Incident Response Plan Operating Procedure* and *Cyber Playbook.*
- Conducted an incident response exercise to assess its incident response capabilities.
- Demonstrated progress in implementing advanced requirements for event logging.

[6] See Appendix A, Tables 2 and 3, for the definitions and explanations of the CSF functions and domains and the IG FISMA Reporting Metrics maturity levels, respectively.

- Finalized its *Supply Chain Strategic Plan* and *Supply Chain Risk Management Operating Procedure.*

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 Has Not Developed CSF Profiles (**Finding 1**: Govern Function – Cybersecurity Governance Domain).
- The DNFSB Did Not Collect Software Self-Attestation Forms for All Software (**Finding 2**: Govern Function – Cybersecurity Supply Chain Risk Management Domain).
- The DNFSB Did Not Maintain a Comprehensive Inventory of Data and Metadata (**Finding 3**: Identify Function – Risk and Asset Management Domain).
- The DNFSB Did Not Conduct an Annual Security Control Assessment and Maintain Up-to-Date Security Assessment Documentation for the GSS (**Finding 4**: Detect Function – Information Security Continuous Monitoring Domain).

In addition, the DNFSB has outstanding prior-year recommendations that impact the IG FISMA Reporting Metrics. Specifically, at the beginning of FY 2025, the DNFSB had 18 open recommendations from prior FISMA evaluations and audits dating from 2019 through 2024. During our FY 2025 audit, we determined that the DNFSB took corrective actions to address 12 of these recommendations, and we consider those recommendations closed. Corrective actions are in progress for the six recommendations that remain open.[7]

To fully progress toward a "Managed and Measurable" maturity level, the DNFSB will need to address new and repeated weaknesses in its security program related to the following domains of the IG FISMA Reporting Metrics: Cybersecurity Governance, Cybersecurity Supply Chain Risk Management, Risk and Asset Management, Configuration Management,[8] Identity and Access Management, Data Protection and Privacy, Information Security Continuous Monitoring, and Contingency Planning. As such, to implement an effective information security program, we encourage the DNFSB to focus on implementing controls and processes related to the core metrics and addressing weaknesses noted in this report. A focus on the core metrics will help the DNFSB align its information security program with administration priorities, high-impact security processes, and the essential functions necessary to determine security program effectiveness.

As a result of the weaknesses noted in this audit, we made seven new recommendations to assist the DNFSB in strengthening its information security program and practices. Additionally, six prior-year recommendations remain open.[9]

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.
[8] DNFSB has numerous ongoing plans of action and milestones (POA&Ms) related to remediating vulnerabilities. Since DNFSB is managing vulnerabilities on a case-by-case basis and has existing POA&Ms, a new finding was not issued.
[9] See Appendix C for the status of prior-year recommendations.

II. 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 CSF 2.0.

Security Function: Govern

The objective of the Govern function is to establish, communicate, and monitor an organization's cybersecurity risk management strategy, expectations, and policy. We determined that the maturity level of the DNFSB's Govern function is Level 2: *Defined*.

Cybersecurity Governance

An agency with an effective cybersecurity governance program (1) monitors and reports on its progress in reaching target profiles and refines its organizational profiles periodically based on known risk exposure; (2) uses qualitative and quantitative data to assess the effectiveness of its cybersecurity risk management and integrates the cybersecurity risk management program into the organization's enterprise risk management strategy; and (3) ensures that it has allocated adequate resources commensurate with cybersecurity responsibilities and uses qualitative and quantitative performance measures on the effectiveness of cybersecurity risk management roles.

We determined that the maturity level of the DNFSB's Cybersecurity Governance domain is Level 2: *Defined.* We identified weaknesses in the DNFSB's Cybersecurity Governance domain related to developing CSF profiles (refer to **Finding 1** below) and completing an annual security control assessment and maintaining up-to-date security assessment documentation for the GSS (refer to **Finding 4** below).

Finding 1: The DNFSB Has Not Developed CSF Profiles

The DNFSB has not developed a CSF project plan and/or procedures for using NIST CSF 2.0[10] (February 26, 2024), including guidance for activities such as developing and maintaining both current and target cybersecurity profile(s).[11]

The DNFSB Chief Information Security Officer stated that the DNFSB developed its existing IT security program policies and procedures to align with NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* and the detailed control implementation requirements contained in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.* However, DNFSB IT management determined that the release of NIST CSF 2.0 provided an opportunity to begin leveraging the CSF as a framework to evaluate the effectiveness of the DNFSB's information security program, as this would provide better

[10] See NIST CSF 2.0 online here.
[11] NIST CSF 2.0 (February 26, 2024) provides guidance to assist with managing cybersecurity risks. Section 3.1 offers guidance on the use of cybersecurity profiles to understand, tailor, assess, prioritize, and communicate cybersecurity objectives. A CSF organizational profile describes an organization's current and/or target cybersecurity posture in terms of the CSF core's outcomes. The CSF core is a taxonomy of high-level cybersecurity outcomes that can help organizations manage their cybersecurity risks. The CSF core components are a hierarchy of functions, categories, and subcategories that detail each outcome.

alignment with the FISMA IG Metrics, which are closely aligned to the CSF. As a result, the DNFSB is finalizing a project plan and procedures for developing and maintaining current and target CSF profiles.

Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), states:

> *Each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework)*[12] *developed by NIST, or any successor document, to manage the agency's cybersecurity risk.*

The absence of current and target CSF profiles increases the risk that the DNFSB may not appropriately plan for or address cybersecurity risks. It may also increase the risk that a bad actor may exploit breaches, system interruptions, and vulnerabilities.

Recommendation 1: We recommend that the DNFSB finalize its project plan and procedures for developing and maintaining current and target CSF profiles.

Recommendation 2: We recommend that the DNFSB develop current and target CSF profiles.

Cybersecurity Supply Chain Risk Management

An agency with an effective cybersecurity supply chain risk management program (1) reports qualitative and quantitative performance measures on the effectiveness of its supply chain risk management program, and (2) has incorporated supplier risk evaluations into its continuous monitoring practices.

We determined that the maturity level of the DNFSB's Cybersecurity Supply Chain Risk Management domain is Level 2: *Defined*. Specifically, we have seen improvement in the DNFSB's Cybersecurity Supply Chain Risk Management domain as a result of the DNFSB finalizing its *Supply Chain Strategic Plan* and *Supply Chain Risk Management Operating Procedure*. However, we identified a new weakness in this domain related to collecting software self-attestation forms from software providers (refer to **Finding 2** below). Further, we noted that the DNFSB has three open prior-year recommendations[13] related to conducting a supply chain risk assessment and establishing and monitoring performance metrics in service level agreements (SLAs) related to contractor systems.

Finding 2: The DNFSB Did Not Collect Software Self-Attestation Forms for All Software

As required by OMB Memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (June 9, 2023), we noted that the DNFSB did not collect the DHS Cybersecurity and Infrastructure

[12] Before version 2.0, the Cybersecurity Framework was called the *Framework for Improving Critical Infrastructure Cybersecurity*. This title is not used for NIST CSF 2.0.
[13] Recommendations 2 and 3, *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, March 25, 2021) and Recommendation 3, *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, March 31, 2020). See Appendix C for additional information regarding these prior-year recommendations.

Agency (CISA) Secure Software Development Attestation Forms[14] for all of the software end products that it used. Specifically, we reviewed DNFSB's Software Attestation List Tracker and found that the DNFSB did not obtain completed software attestation forms from 3 out of 61 software producers. In addition, the DNFSB did not request an extension or a waiver from OMB, nor did it document a plan for mitigating any potential risk it incurred as a result of not fully complying with OMB M-23-16.

A DNFSB official stated that the DNFSB has contacted the software producers repeatedly and has been unable to obtain evidence of compliance with the NIST Secure Software Development Framework (SSDF) or applicable plans of actions and milestones (POA&Ms) for two of the three software producers. The remaining software producer did not show compliance through a completed Secure Software Development Attestation Form; instead, it provided certification of compliance with a different standard.

OMB Memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (June 9, 2023), states:

> *Executive Order (EO) 14028, Improving the Nation's Cybersecurity (May 12, 2021), focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs agencies to take a variety of actions that "enhance the security of the software supply chain." In accordance with the EO, the National Institute of Standards and Technology (NIST) has released the NIST Secure Software Development Framework (SSDF), SP 800-218, and the NIST Software Supply Chain Security Guidance (hereinafter, referred to collectively as "NIST Guidance"). OMB Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-22-18) (September 14, 2022), requires agencies to comply with that NIST Guidance. Pursuant to M-22-18, agencies must only use software that is provided by software producers who can attest to complying with Government-specified minimum secure software development practices.*
>
> *This memorandum reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and extends the timelines for agencies to collect attestations from software producers. Additionally, this memorandum provides supplemental guidance on the scope of M-22-18's requirements and on agencies' use of plan of actions and milestones (POA&Ms) when a software producer cannot provide the required attestation, but plans to do so. To the extent any provision of this memorandum may be read to conflict with any provision of M-22-18, this memorandum is controlling.*

Further, OMB Memorandum M-23-16 contains the following requirements:

- Agencies must collect attestations from the producers of software end products the agency uses because the producer of that end product is best positioned to ensure the security of the product.

[14] The DHS CISA Secure Software Development Attestation Form Instructions indicate that the self-attestation form identifies the minimum secure software development requirements a software producer must meet, and attest to meeting, before federal agencies may use software subject to the requirements of OMB Memoranda M-22-18 and M-23-16. Software producers use this form to attest that they developed their software in conformity with specified secure software development practices.

- If a software producer cannot attest to one or more of the practices identified in the attestation form, an agency may still use the software if the producer identifies the practices to which it cannot attest, documents practices it has in place to mitigate the associated risks, and submits a satisfactory POA&M.
- The producer of a given software application must identify the practices to which it cannot attest, document practices it has in place to mitigate associated risks, and submit a POA&M to the agency. If the agency finds the documentation satisfactory, it may continue using the software but must concurrently seek an extension of the deadline for attestation from the OMB. Extension requests submitted to the OMB must include a copy of the software producer's POA&M.

Without Secure Software Development Attestation Forms, or POA&Ms for security software practices to which the software producers cannot attest, the DNFSB cannot ensure that the software it uses complies with NIST's specified secure software development practices. As such, the DNFSB may be at an increased risk of using less-secure software that may expose its systems and networks to vulnerabilities and exploits by bad actors.

In addition, without requesting an extension or a waiver from the OMB and documenting a plan for mitigating any potential risk of noncompliance with the OMB's software attestation requirements, the DNFSB is not in full compliance with the OMB Memorandum M-23-16 requirements.

Recommendation 3: We recommend that the DNFSB coordinate with its software producers to obtain Secure Software Development Attestation Forms. If the DNFSB is unable to obtain the attestation forms, it should request POA&Ms from the software producers, in accordance with OMB Memorandum M-23-16.

Recommendation 4: We recommend that the DNFSB submit POA&Ms and risk-based waiver requests to OMB for approval in accordance with OMB Memorandum M-23-16.

Security Function: Identify

The objective of the Identify function is to ensure that the organization understands its cybersecurity risks. We determined that the maturity level of the DNFSB's Identify function is Level 3: *Consistently Implemented*.

Risk and Asset Management

An agency with an effective risk and asset 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 and asset management program.

We determined that the maturity level of the DNFSB's Risk and Asset Management domain is Level 3: *Consistently Implemented*. The DNFSB demonstrated strengths in this area by finalizing its *Enterprise Architecture* document and employing automation to help track hardware and software assets. However, we identified new weaknesses in the DNFSB's Risk and Asset Management domain related to maintaining a comprehensive inventory of data and metadata (refer to **Finding 3** below) and completing an annual security control assessment and

maintaining up-to-date security assessment documentation for the GSS (refer to **Finding 4** below).

Additionally, we noted that the DNFSB has three open prior-year recommendations[15] related to assessing enterprise-level and business process-level risk as part of its enterprise risk management program, implementing a centralized view of risk across the organization, and implementing formal procedures to prioritize and track POA&Ms.

Finding 3: The DNFSB Did Not Maintain a Comprehensive Inventory of Data and Metadata

The DNFSB has not developed a comprehensive and accurate inventory of its data and corresponding metadata.[16]

DNFSB management stated that the DNFSB has not documented policies and procedures for developing and maintaining an inventory of its data and metadata. Specifically, during the DNFSB's ongoing effort to complete its internal self-assessment of its information security program using NIST CSF 2.0, the IT team identified a lack of inventories of data and corresponding metadata for designated data types and identified this issue as an area to address. Management plans to add this to the FY 2026 work plan, as it does not have sufficient resources to create the required procedures in FY 2025.

OMB Memorandum M-25-05, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance*, states:

> 4. *Agency Requirements that Apply to All Data Assets*
>
> *a. Comprehensive Data Inventories*
>
> *Agencies must, to the maximum extent practicable, develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by the agency (hereinafter "in the possession of the agency"), with the exception of data assets contained on a national security system. Data assets that are in the possession of, or shared by, more than one agency are required to be listed independently by each agency possessing those assets on the agency's comprehensive data inventory. Agencies must ensure that the comprehensive data inventory is clear and allows the public to understand all data assets in the possession of the agency.*
>
> *The following requirements apply to comprehensive data inventories:*
>
> ***i. Interoperable with the Federal Data Catalog**. General Services Administration (GSA) is responsible for developing and maintaining the Federal Data Catalog, a centralized public online interface dedicated to*

[15] Recommendations 2 and 3, *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, March 25, 2021) and Recommendation 3, *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, March 31, 2020). See Appendix C for additional information regarding these prior-year recommendations.

[16] OMB Memorandum M-25-05, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance*, defines metadata as "structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions."

sharing agency data assets with the public. As part of its responsibilities, GSA updates and maintains the requirements and schema established by OMB and made publicly available through Data.gov or any successor website. Agency comprehensive data inventories must be interoperable with the Federal Data Catalog as described in Section 5(b) of this Memorandum to ensure that agency information is extracted correctly and displayed there appropriately. The comprehensive data inventory must be maintained in an open format consistent with the ISO/IEC 21778:2017, commonly known as the JavaScript Object Notation (JSON) format, or a successor format.

ii. ***Metadata.*** *Each agency's comprehensive data inventory must conform to the standard metadata schema approved by OMB and available on resources.data.gov. If that schema changes, agencies must update their inventories appropriately within one year.*

The absence of policies and procedures for creating and maintaining a comprehensive and accurate inventory of DNFSB data and corresponding metadata increases the risk that the DNFSB may not properly account for and secure sensitive data.

Recommendation 5: We recommend that the DNFSB document policies and procedures for developing and maintaining a comprehensive and accurate inventory of data and the corresponding metadata for the DNFSB's data types.

Recommendation 6: We recommend that the DNFSB create and maintain a comprehensive inventory of data and corresponding metadata.

Security Function: Protect

The objective of the Protect function is to ensure that organizations use safeguards to manage their cybersecurity risks. We determined that the maturity level of the DNFSB's Protect function is Level 3: *Consistently Implemented*.

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; 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 2: *Defined*. We noted that while DNFSB has shown some improvements in its vulnerability management program by implementing a process to manage vulnerabilities on a case-by-case basis, the DNFSB continues to have numerous ongoing POA&Ms related to remediating aged vulnerabilities.

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 and uses automated mechanisms to assist in managing privileged accounts.

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 making progress in 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 an opportunity to improve its identity and access management program by implementing one open prior-year recommendation in this area.[17] The recommendation is related to the 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 throughout its life cycle (i.e., at rest, in transit, and through destruction) and monitoring inbound and outbound traffic. However, we noted that the DNFSB has one open prior-year recommendation in this area related to developing role-based privacy training.[18]

Security Training

An agency with an effective security training program identifies and addresses gaps in security knowledge, skills, and abilities through training or talent acquisition.

We determined that the maturity level of the DNFSB's Security Training domain is Level 3: *Consistently Implemented*. We have seen improvements in the DNFSB's Security Training domain related to personnel completing privacy awareness and literacy training and maintaining the records in the DNFSB's Learning Management System. However, we noted that the DNFSB performed a workforce assessment, and identified a need related to an Information System Security Officer (ISSO) position. DNFSB has included the ISSO position in its budget. However, at the time of testing, DNFSB had not filled the ISSO position through training or talent acquisition.[19]

Security Function: Detect

The objective of the Detect function is to ensure that organizations identify and analyze possible cybersecurity attacks and compromises. We determined that the maturity level of the DNFSB's Detect function is Level 3: *Consistently Implemented*.

[17] Recommendation 9, *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, March 25, 2021). See Appendix C for additional information regarding these prior-year recommendations.
[18] 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, December 21, 2021). See Appendix C for additional information regarding these prior-year recommendations.
[19] Since the ISSO position has been funded, just not filled, a new finding was not issued.

Information Security Continuous Monitoring

An agency with an effective information security continuous monitoring program maintains ongoing authorizations of information systems; uses up-to-date cyber threat intelligence when analyzing logs; automates its inventory collection and anomaly detection to detect unauthorized devices; 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 of the DNFSB's Information Security Continuous Monitoring domain is Level 3: *Consistently Implemented*. The DNFSB demonstrated strengths in this area by using cyber threat intelligence in its log analysis tools to improve the accuracy of its detections and to characterize threat actors, their methods, and indicators of compromise.

However, we noted that the DNFSB has two open prior-year recommendations in this area related to establishing performance metrics to more effectively manage and optimize all domains of the DNFSB's information security program.[20] Additionally, the DNFSB's information security continuous monitoring program needs improvement, as noted below.

Finding 4: The DNFSB Did Not Conduct an Annual Security Control Assessment and Maintain Up-to-Date Security Assessment Documentation for the GSS

The DNFSB did not conduct an annual security control assessment for the GSS. Additionally, the DNFSB did not review and update its security assessment documentation annually in accordance with the *DNFSB Risk Management Framework Handbook*. Specifically, the DNFSB last updated its security assessment documentation as follows:

- System Security Plan: February 8, 2023.
- Security Assessment Report: June 16, 2023.
- Information System Contingency Plan: December 7, 2023.
- Privacy Impact Assessment: April 7, 2023.

DNFSB management stated that the DNFSB had prioritized updating and creating documents that were related to closing open FISMA recommendations and meeting new external requirements. The DNFSB plans to update the identified documents by the end of FY 2025.

The *DNFSB Risk Management Framework Handbook* (January 9, 2024), section 9.3, states that the DNFSB must review and update these documents as follows:

- *System Security Plan - Review/update annually or when major changes are implemented.*
- *Information System Contingency Plan - Review/update annually or when major changes are implemented.*
- *Privacy Impact Assessment - Review/update annually, or if changes to Personally Identifiable Information (PII) occur.*
- *Security Assessment Report - Review/update based on annual security controls testing.*

[20] Recommendation 3, *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, March 25, 2021) and Recommendation 3, *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, March 31, 2020). See Appendix C for additional information regarding these prior-year recommendations.

Without conducting annual security control assessments and maintaining up-to-date security documentation, the DNFSB does not have reasonable assurance that controls are operating effectively, which may expose the DNFSB to information loss, fraud, or abuse. In addition, the lack of timely assessments and/or continuous monitoring limits authorizing officials' ability to make effective decisions regarding the risk for compromise created by system operations.

Recommendation 7: We recommend that the DNFSB prioritize and conduct an annual security control assessment and update the GSS' System Security Plan, Security Assessment Report, Privacy Impact Assessment, and Information System Contingency Plan in accordance with the *DNFSB Risk Management Framework Handbook.*

Security Function: Respond

The objective of the Respond Function is to ensure that organizations take action regarding a detected cybersecurity incident. We determined that the maturity level of the DNFSB's Respond function is Level 5: *Optimized*.

Incident Response

An agency with an effective incident response program:

- Uses 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.
- Uses 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.
- Meets event logging maturity requirements.

We determined that the maturity level of the DNFSB's Incident Response domain is Level 5: *Optimized*. The DNFSB has demonstrated improvements in this area related to updating its *Incident Response Plan Operating Procedure* and *Cyber Playbook,* conducting an incident response exercise to assess its incident response capabilities, and making progress in implementing advanced requirements for event logging.

Security Function: Recover

The objective of the Recover function is to ensure that organizations restore assets and operations affected by a cybersecurity incident. 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 ensures that it integrates the results of business impact analyses (BIAs) with its enterprise risk management processes and uses these results to make senior-level decisions; employs automated mechanisms to thoroughly and

effectively test system contingency plans; and communicates metrics on the effectiveness of recovery activities to relevant stakeholders.

We determined that the maturity level of the DNFSB's Contingency Planning domain is Level 3: *Consistently Implemented.* The DNFSB has demonstrated strengths in this area by implementing backup and recovery controls. However, we identified a new weakness in the DNFSB's Contingency Planning domain related to updating the GSS Information System Contingency Plan on an annual basis (refer to **Finding 4** above). Further, we noted that the DNFSB has one open prior-year recommendation[21] in the Contingency Planning domain related to performing a BIA on a timely basis.

[21] Recommendation 23, *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, December 21, 2021). 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 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 the minimum information security requirements necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with the Federal Information Processing Standards issued by NIST. In addition, NIST develops and issues SPs 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 January 15, 2025, the OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum provides reporting guidance for FY 2025 in accordance with FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. As a result, the OMB, CIGIE, and other stakeholders collaborated to develop these metrics.

One of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving objectives that strengthen federal cybersecurity. The FY 2025 IG FISMA Reporting Metrics were updated to reflect recent developments:

- NIST published CSF 2.0 in February 2024, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's enterprise risk management strategy. As such, a new IG FISMA function *(Govern)* was added that includes a new domain (*Cybersecurity Governance)* to align with NIST CSF 2.0.
- To align with NIST CSF 2.0, the Supply Chain Risk Management domain moved from the *Identify* function to the *Govern* function, to better reflect agency oversight of supply chain risk.
- A new domain, Risk and Asset Management, was introduced in the Identify function to group metrics on system inventory and hardware, software, and data management.
- Five supplemental metrics are in scope for the FY 2025 IG FISMA evaluation, including two new supplemental metrics that are focused on system-level risk management practices critical to achieving Zero Trust Architecture objectives.
- The core metric on information system-level risk management was revised to focus on the maturity of agencies' implementation of the NIST Risk Management Framework.

As highlighted in **Table 2**, the FY 2025 IG FISMA Reporting Metrics are designed to assess the maturity of an agency's information security program and practices and align with the six function areas in NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover.

Table 2: Alignment of the CSF Functions to the Domains in the FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	Cybersecurity Governance and Cybersecurity Supply Chain Risk Management
Identify	The organization's current cybersecurity risks are understood.	Risk and Asset Management
Protect	Safeguards to manage the organization's cybersecurity risks are used.	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	Information Security Continuous Monitoring
Respond	Actions regarding a detected cybersecurity incident are taken.	Incident Response
Recover	Assets and operations affected by a cybersecurity incident are restored.	Contingency Planning

Source: Sikich's analysis of NIST CSF 2.0 and the FY 2025 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 at least 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 the policies and procedures 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 2025 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

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 2025. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, supporting the FY 2025 IG FISMA Reporting Metrics, for the DNFSB GSS (**Table 4**).

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

For this year's review, IGs were required to assess 20 core and 5 supplemental IG FISMA Reporting Metrics across 6 function areas—Govern, 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 audit also included an evaluation of whether the DNFSB took corrective actions to address open recommendations from the FY 2024 FISMA audit,[22] FY 2023 FISMA audit,[23] FY 2021 FISMA evaluation,[24] FY 2020 FISMA evaluation,[25] and FY 2019 FISMA evaluation.[26]

The audit covered the period from October 1, 2024, through June 30, 2025. We performed audit fieldwork from January to June 2025.

Methodology

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

[22] *Audit of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024* (Report No. DNFSB-24-A-05, September 30, 2024).
[23] *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, September 29, 2023).
[24] *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, December 21, 2021).
[25] *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, March 25, 2021).
[26] *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, March 31, 2020).

To accomplish our audit objectives, 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 2025.
- Focused our testing activities on assessing the maturity of the 20 core and 5 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Performed inquiries and walkthroughs with DNFSB management and staff.
- Considered guidance contained in OMB's Memorandum M-25-04, *Fiscal Year 2025 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 1 internally maintained DNFSB information system from the 36 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 Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- 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 2023-2024 IG FISMA Reporting Metrics* introduced a calculated average scoring model that was continued for the FY 2025 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 2025 IG FISMA Reporting Metrics guidance[27] to form our conclusions for each CSF 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

[27] The FY 2025 IG FISMA Reporting Metrics provide the agency IG with the discretion to determine the rating for each of the CSF 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.

FISMA Reporting Metrics and progress that the DNFSB has made in addressing outstanding prior-year recommendations, to form our risk-based conclusion.

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 2024 FISMA audit, FY 2023 FISMA audit, FY 2021 FISMA evaluation, FY 2020 FISMA evaluation, and FY 2019 FISMA evaluation.[28] At the time of testing and IG FISMA Reporting Metric submission, 6 of the 18 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[29]
DNFSB-24-A-05 FY 2024 FISMA Audit **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*.	The DNFSB requested closure of this recommendation. The DNFSB approved operating procedure (OP)-411.1-16, *System and Information Integrity Operating Procedure,* on September 17, 2024, which replaces OP-412.2-1, *Vulnerability Management*. The DNFSB is currently organizing the vulnerability data to create a vulnerability POA&M in accordance with OP-411.1-16.	**Closed.** The OIG[30] verified the evidence that DNFSB management provided to support implementation of OP-411.1-16, *System and Information Integrity 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, as well as the vulnerability POA&Ms created in accordance with OP-411.1-16.	**Configuration Management Domain**

[28] See footnotes 22, 23, 24, 25, and 26.
[29] All prior-year recommendations were mapped to specific affected IG FISMA Reporting Metric domains based upon the nature of each recommendation. In some cases, the nature of the recommendation may affect multiple domains.
[30] Through the OIG's Status of Recommendations process, the OIG has closed various recommendations. This is indicated in the Auditor's Position on Status field.

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[29]
	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.			
DNFSB-24-A-05 FY 2024 FISMA Audit **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*.	The DNFSB requested closure of this recommendation. The DNFSB updated its delivery method for IT training.	**Closed.** The OIG verified the evidence that DNFSB management provided and confirmed that the DNFSB has completed training through AgLean Learning Management System in accordance with the *DNFSB Awareness and Training Program Standard Operating Procedure*.	**Security Training Domain**
DNFSB-24-A-05 FY 2024 FISMA Audit **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.	The DNFSB requested closure of this recommendation. The DNFSB updated the *Incident Response Plan* and *Incident Response Process Guide Cyber Playbook*.	**Closed.** The OIG verified the evidence that DNFSB management provided and confirmed that the DNFSB completed updates to the *Incident Response Plan* and *Incident Response*	**Incident Response Domain**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[29]
			Process Guide Cyber Playbook.	
DNFSB-24-A-05 FY 2024 FISMA Audit **Recommendation 4**	We recommend that the DNFSB ensure all personnel with incident response responsibilities participate in incident response exercises.	The DNFSB requested closure of this recommendation. The DNFSB held an annual incident response exercise and included applicable parties.	**Closed.** The OIG verified that the DNFSB completed incident response and breach response training exercises for personnel defined in OP-411.1-21, *Incident Response Plan Operating Procedure.*	**Incident Response Domain**
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).	The DNFSB requested closure of this recommendation. The DNFSB has completed implementation of required logging for Critical Levels 1, 2, and 3, as required by OMB Memorandum M-21-31.	**Closed** We conducted a walkthrough of the DNFSB's Event Logging and noted that the DNFSB implemented event logging requirements to meet the required logging for Critical Levels 1, 2, and 3, as required by OMB Memorandum M-21-31.	**Incident Response**
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	The DNFSB requested closure of this recommendation. The DNFSB completed and approved its *Supply Chain Strategic Plan* and *Supply Chain Risk Management Operating Procedure* on March 21, 2025, and May 1, 2025, respectively.	**Closed** We inspected the *Supply Chain Strategic Plan* and *Supply Chain Risk Management Operating Procedure* and determined that the DNFSB has developed policies and procedures for (a) managing supply chain risks across the agency; (b)	**Cybersecurity Supply Chain Risk Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[29]
	compliance with defined cybersecurity and supply chain requirements; and c. How counterfeit components are prevented from entering the DNFSB supply chain.		ensuring that its monitoring of external providers complies with defined cybersecurity and supply chain requirements; and (c) preventing counterfeit components from entering the DNFSB supply chain.	
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 Identity Credential Access Management (ICAM) architecture and OMB Memorandum (M)-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation program.	The DNFSB requested closure of this recommendation. The DNFSB completed and approved its *Enterprise Architecture* and *Identification and Authentication Operating Procedures* on December 17, 2024, and September 17, 2024, respectively.	**Closed** We inspected the *Enterprise Architecture* and *Identification and Authentication Operating Procedures* and determined that the DNFSB has made updates to reflect the implementation of strong authentication requirements.	**Identity and Access Management**
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.	This recommendation remains open. **Estimated target completion date: FY 2025 Q4** The DNFSB is currently in the process of developing role-based privacy training.	**Open** The DNFSB continues to work toward closure. The DNFSB has identified training for those with significant privacy/data protection duties and is currently finalizing the training in AgLearn. The DNFSB has added requirements related to taking this training to the most recent draft of OP-411.1-2: *Security and Privacy Awareness and Training Operating Procedures,* which is currently under review by management.	**Data Protection and Privacy**
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	This recommendation remains open.	**Open** We inspected the documentation provided in	**Contingency Planning**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[29]
	strategy and mitigation planning activities.	**Estimated target completion date: FY 2025 Q4** The DNFSB continues to work toward closure and has established a BIA working group to complete this task.	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 1**	Define an Information Security Architecture (ISA) in accordance with the *Federal Enterprise Architecture Framework*.	The DNFSB requested closure of this recommendation. The DNFSB has incorporated ISA into its *Enterprise Architecture* document.	**Closed** The OIG verified that the DNFSB has defined an ISA in accordance with the Federal Enterprise Architecture Framework.	**Risk and Asset 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 2026** The DNFSB continues to work toward closure. It has included the ISA in its *Enterprise Architecture* document. It also completed a cybersecurity risk register, including information system-level risks, in February 2025. However, assessment of enterprise-level and business process-level risks will be part of the enterprise risk management program. Documentation for this program is under review by management. The enterprise risk management documentation will define risk tolerance and appetite levels. Once the enterprise risk management documentation is	**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 and Asset Management** **Cybersecurity Supply Chain Risk Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[29]
		complete, the DNFSB can use the risk definitions to conduct organization-wide security and privacy risk assessments.		
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 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.	This recommendation remains open. **Estimated target completion date: FY 2026** DNFSB management stated that they continue to work toward closure. The DNFSB has established SLA metrics but is currently in the process of refining them. The DNFSB is also in the process of establishing an enterprise risk management program, which will provide a centralized view of risk across the organization. The Directive and operating procedures are currently under review by management. The DNFSB has drafted a POA&M operating procedure that is also currently under review by management.	**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 and Asset Management** **Cybersecurity Supply Chain Risk Management** **Information Security Continuous Monitoring**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[29]
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 2025 Q3** The DNFSB continues to work toward closure. The DNFSB cyber team has conducted a risk assessment on automated management of privileged accounts and found the risk to be too great to implement. A formal risk acceptance memorandum is currently under review by management.	**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 11**	Conduct the agency's annual breach response plan exercise for FY 2021.	The DNFSB requested closure of this recommendation. The DNFSB conducted an annual breach response plan exercise in September 2024.	**Closed** The OIG verified that the DNFSB has conducted its annual breach response exercise plan.	**Data Protection and Privacy**
DNFSB-20-A-05 FY 2019 FISMA Evaluation **Recommendation 3**	b. Collaborate with the 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.	**Recommendation 3a: Closed in FY 2024.** **Recommendations 3b-3d: Open** **Estimated target completion date: FY 2025**. The DNFSB continues to work toward closure. It has established SLA metrics but is currently in the process of refining these metrics. The DNFSB is also in the process of establishing an enterprise risk management program, which will provide a centralized view of risk across the organization. The Directive and operating procedure are	**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.	**Cybersecurity Supply Chain Risk Management** **Information Security Continuous Monitoring** **Risk and Asset Management**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[29]
	d. Implement a centralized view of risk across the organization.	currently under review by management.		
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.	The DNFSB requested closure of this recommendation. The DNFSB has revised its *Configuration Management Plan* to include a requirement for remedial training and consequences for failure to follow the appropriate processes.	**Closed** We inspected the *Configuration Management Operating Procedure* and *Configuration Management Plan* and determined that the DNFSB incorporated requirements for remedial training.	**Configuration Management**
DNFSB-20-A-05 FY 2019 FISMA Evaluation **Recommendation 8**	Continue efforts to meet milestones of the DNFSB ICAM [Identity, Credential, and Access Management] Strategy necessary for fully transitioning to DNFSB's "to-be" ICAM architecture.	The DNFSB requested closure of this recommendation. The DNFSB published its *Enterprise Architecture* document—which includes the agency's "to-be" ICAM architecture—in December 2024 and published OP 411.1-7, *Identification and Authentication Operating Procedures,* in September 2024.	**Closed** The OIG reviewed the *Enterprise Architecture* document and OP 411.1-7, *Identification and Authentication Operating Procedures,* and verified that the DNFSB has met the milestones of its ICAM strategy necessary for the DNFSB to fully transition to its "to-be" ICAM architecture.	**Identity and Access Management**
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 [Information and Communications Technology] supply chain risk.	The DNFSB requested closure of this recommendation. The *DNFSB GSS Information Systems Contingency Plan* states that the DNFSB discusses supply chain risk management in the *Supply Chain Strategic Plan* and *Supply Chain Risk Management Operating Procedure.*	**Closed** We inspected the *DNFSB GSS Information Systems Contingency Plan, Supply Chain Strategic Plan,* and *Supply Chain Risk Management Operating Procedure,* and noted that the contingency plan references the supply chain risk management plans and procedures. We also noted	**Cybersecurity Supply Chain Risk Management** **Contingency Planning**

Report No. Recommendation No.	Recommendation	DNFSB's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[29]
			that the DNFSB discusses supply chain risk management in the *Supply Chain Strategic Plan* and *Supply Chain Risk Management Operating Procedure*.	

APPENDIX D: MANAGEMENT RESPONSE

DNFSB management reviewed a discussion draft of this report. On September 2, 2025, DNFSB management concurred with the findings and recommendations of this report and chose not to provide formal comments for inclusion in this report.