MEMORANDUM

DATE: November 1, 2023

TO: Katherine Herrera
Acting Executive Director of Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021 (DNFSB-22-A-04)

REFERENCE: ASSOCIATE DIRECTOR FOR BOARD OPERATIONS, DEFENSE NUCLEAR FACILITIES SAFETY BOARD, CORRESPONDENCE DATED SEPTEMBER 20, 2023

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated September 20, 2023. Based on this response, recommendations 5, 6, 12 to 19, and 21 are closed, and recommendations 1 to 4, 7 to 11, 20, and 22 to 24 remain open and resolved. Please provide an updated status of all recommendations by **March 31, 2024**.

If you have any questions or concerns, please call me at 301.415.1982 or Terri Cooper, Team Leader, at 301.415.5965.

Attachment:
As stated

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

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 1:	Update the ISA and use the updated ISA to: a. Assess enterprise, business process, and information system level risks; b. Update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.
Agency Response Dated September 20, 2023:	a) A centralized view of risk across the organization will be possible once the agency implements an Enterprise Risk Management Program, which is currently under development with an outside consultant. b) Risk tolerance, risk profiles and a risk register will be established as part of DNFSB's ERM program. Risks from the information system level will flow up to the business process level, and risks at the business process level will flow up to the enterprise level to allow management to make more informed risk management decisions.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates the Information Security Architecture (ISA) to assess risk and update risk tolerance and appetite levels necessary for prioritizing and guiding risk management on the enterprise, business process, and information system levels.
Status:	Open: Resolved.

Recommendation 2:	Using the results of recommendations one above: a. Utilizing guidance from the National Institute of Standards in Technology (NIST) Special Publication (SP) 800-55 (Rev. 1) – *Performance Measurement Guide for Information Security* to establish performance metrics to manage and optimize all domains of the DNFSB information security program more effectively; b. Implement a centralized view of risk across the organization; c. Implement formal procedures for prioritizing and tracking POA&Ms to remediate vulnerabilities.
Agency Response Dated September 20, 2023:	a) DNFSB will review existing policies & procedures against the recommendations in NIST SP-800 55 Rev.2 and make any updates by Q2 FY 2024. b) A centralized view of risk across the organization will be possible once the agency implements an Enterprise Risk Management Program, which is currently under development with an outside consultant. c) DNFSB will update its Risk Management Framework Handbook and its and Continuous Monitoring Policies & Procedures Guide to include prioritization of vulnerabilities based on severity level by Q2 FY 2024.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates the ISA to utilize guidance from NIST to establish metrics to manage and optimize all domains of the DNFSB information security program more effectively; implements a centralized view of risk across the organization; and, implements formal procedures for prioritizing and tracking plan of actions and milestones (POA&Ms) to remediate vulnerabilities.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 3:	Update the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, to include: a. Defining a frequency for conducting Risk Assessments to periodically assess agency risks to integrate results of the assessment to improve upon mission and business processes.
Agency Response Dated September 20, 2023:	DNFSB published the Risk Assessment Policy in January 2023, which included defined frequencies for risk assessments and integrating those results into mission and business processes. As part of the external security assessment of the GSS, a risk assessment and control assessment were performed by an external auditor. DNFSB completed an external security assessment in June of 2023 and issued an updated ATO for the DNFSB GSS in July 2023. Based on actions already taken, DNFSB's position is that this recommendation needs to be closed.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, including 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.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

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; c. How counterfeit components are prevented from entering the DNFSB supply chain.
Agency Response Dated September 20, 2023:	Supply Chain Risk will be addressed in an upcoming Supply Chain Risk Management Program Operating Procedure. The estimated completion is Q4 FY 2023.
OIG Analysis:	The OIG will close this recommendation when the DNFSB defines a supply chain risk management strategy to drive the development and implementation of policies and procedures for the items in bullets a. through c. above.
Status:	Open: Resolved.

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.
Agency Response Dated September 20, 2023:	DNFSB required all members of the IT Team that are authorized to submit change request tickets to take remedial "CCB and Change Request Training" in August 2022 and then take an updated remedial training in December 2022 that addressed changes to the CCB & SIA form process. Based on actions already taken, DNFSB's position is that this recommendation needs to be closed.
OIG Analysis:	The OIG noted an improvement in change documentation for our sampled changes during the FIMSA audit. The OIG verified that the DNFSB conducted 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. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 6:	Integrate the Configuration Management Plan with risk management and continuous monitoring programs and utilize lessons learned to make improvements to this plan.
Agency Response Dated September 20, 2023:	DNFSB recently updated its Configuration Management Plan, Continuous Monitoring Policies and Procedures Guide, and Risk Management Framework. These three documents are now integrated. DNFSB will request this recommendation be closed.
OIG Analysis:	The OIG inspected the DNFSB Risk Management Framework Handbook, DNFSB Risk Assessment Policy, and the DNFSB GSS Continuous Monitoring Policies and Procedures Guide and confirmed aspects of configuration management (e.g., baseline compliance, patching, change control, etc.) are integrated with risk management and continuous monitoring programs. This recommendation is closed.
Status:	Closed.

Recommendation 7:	Implement automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.
Agency Response Dated September 20, 2023:	This recommendation is a duplicate of 2020-9. DNFSB has determined that automated management of privileged accounts presents a higher risk than the current manual process of account review. DNFSB has implemented a manual review of account activity based on automated reports sent from the Varonis tool weekly. Administrators review this data and act in accordance with DNFSB policies and procedures. DNFSB will request a risk acceptance for this recommendation by Q4 FY 2023.
OIG Analysis:	The OIG will close this recommendation when the DNFSB implements automated mechanisms to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 8:	Continue efforts to implement data loss prevention functionality for the Microsoft Office 365 environment.
Agency Response Dated September 20, 2023:	DNFSB requests OIG to define the exact milestone required to meet closure of this recommendation. Otherwise, DNFSB will always be making efforts to improve data loss prevention functionality for the Microsoft 365 environment.
OIG Analysis:	In the Status of Open Recommendations provided by DNFSB, the OIG noted that the IT team will continue to work with the Records Management staff in the Division of Operational Services to better define the data loss prevention policies in DNFSB's Office 365 tenant. The OIG will close this recommendation when the DNFSB provides evidence of a defined and enforced data loss prevention policy for the Microsoft Office 365 environment.
Status:	Open: Resolved.

Recommendation 9:	Update agency strategic planning documents to include clear milestones for implementing strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program.
Agency Response Dated September 20, 2023:	DNFSB has defined clear milestones for implementing strong authentication in "Pillar I – Identity" of its Zero Trust Architecture Implementation Plan. DNFSB currently participates in DHS/CISA's CDM Shared Service offering (DEFEND F) and has already implemented all of the available capabilities (hardware asset management, software asset management, configuration settings management, vulnerability management, enterprise mobility management, and endpoint detection & response) and is participating with CDM IDAM capabilities as they are being developed and plan to implement them when they become available. DNFSB requests clarification from the OIG regarding what additional actions need to be taken to close this recommendation.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates agency strategic planning documents for all elements in the recommendation, to include clear milestones for implementing strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 10:	Conduct the agency's annual breach response plan exercise for FY 2021.
Agency Response Dated September 20, 2023:	DNFSB conducted incident response/contingency plan exercises on September 26 &27, 2022 and May 24, 2023, that included testing the agency's breach response plan. DNFSB requests confirmation from the OIG if the exercises performed above resolve this recommendation, and if so, then this recommendation needs to be closed. Based on actions already taken, DNFSB's position is that this recommendation needs to be closed.
OIG Analysis:	The OIG inspected the incident response and contingency planning exercises completed and noted they did not include an evaluation of the breach response plan. The OIG requests DNFSB provide additional information pertaining to the testing of the breach response plan.
Status:	Open: Resolved.

Recommendation 11:	Continue efforts to develop and implement role-based privacy training for users with significant privacy or data protection related duties.
Agency Response Dated September 20, 2023:	DNFSB provides role-based privacy training within its required annual Cyber Awareness training. Topics such as Social Networking, handling of Controlled Unclassified Information (CUI) and Classified data, website use, and Social Engineering are all covered by this training. Each user is required to complete this training prior to accessing DNFSB systems. DNFSB further requires all users to take annual Controlled Unclassified Information (CUI) training, and all Federal employees with DOE clearances must take an annual clearance holder training, both of which address requirements for accessing, storing, and transmitting sensitive information. DNFSB has developed updated privacy training and will deliver it to agency users by the end of Q1 FY 2024. DNFSB needs the OIG to define which roles it feels require additional role-based privacy training in order to resolve this recommendation.
OIG Analysis:	This recommendation will be closed when the OIG verifies that the DNFSB developed and implemented role-based privacy training for users with significant privacy or data protection related duties.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 12:	Formally document requirements and procedures for the completion of role-based training and enforcement methods in place for individuals who do not complete role-based training.
Agency Response Dated September 20, 2023:	DNFSB requested this recommendation be closed in "CLOSURE OF FY21 AND FY22 FISMA AUDIT RECOMMENDATIONS" memo dated 8/19/22. Awaiting OIG validation as part of the FY23 FISMA Audit fieldwork.
OIG Analysis:	The DNFSB Security Awareness Training Policy published in August 2022 formally documents the requirements and procedures for completion of role-based training and enforcement methods for individuals that do not complete it. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 13:	Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.
Agency Response Dated September 20, 2023:	Duplicate of recommendation FY2020-12. DNFSB published updates to the Risk Management Framework Handbook, Configuration Management Policy, and Continuous Monitoring Policies and Procedures Guide in FY 2022 and FY 2023. Using these procedures, the DNFSB issued an Authority to Operate for the GSS in July 2023. DNFSB completed an external security assessment in June of 2023 and issued an updated ATO for the DNFSB GSS in July 2023. Based on actions already taken, DNFSB's position is that this recommendation needs to be closed.
OIG Analysis:	Progress has been made in refining procedures such as the DNFSB GSS Continuous Monitoring Policies and Procedures Guide to support adoption of an ongoing authorization model. The OIG verified the implementation of the updated monitoring and assessment procedures and the authorization of the system. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 14:	Update the DNFSB ISCM policies and procedures clearly defining what needs to be monitored at the system and organization level.
Agency Response Dated September 20, 2023:	Procedures for conducing security control assessments at the system or organization level are included in the "Risk Management Framework Handbook" not the "Continuous Monitoring Policies and Procedures Guide" and DNFSB has updated its Risk Management Framework (RMF) Handbook to refine existing monitoring and assessment procedures to support ongoing authorization of DNFSB information systems more effectively. A draft version of this document was provided to the FISMA auditors during their fieldwork in response to a PBC item request and subsequent updates have been made and is pending formal approval by the DNFSB CIO. DNFSB updated its "Continuous Monitoring Policies and Procedures Guide" and "Risk Management Framework Handbook" on 9/29/22. DNFSB will request closure of this recommendation.
OIG Analysis:	The OIG inspected the DNFSB GSS Continuous Monitoring Policies and Procedures Guide and the DNFSB Risk Management Framework Handbook and noted that DFNSB has updated its policies and procedures to clearly define what needs to be monitored at the system and organization level. This recommendation is closed.
Status:	Closed.

Recommendation 15:	Define standard operating procedures for the use of the agency's continuous monitoring tools or update the continuous monitoring plan to include the use of new monitoring tools.
Agency Response Dated September 20, 2023:	DNFSB updated its "Continuous Monitoring Policies and Procedures Guide" to document the specific monitoring tools in use. DNFSB anticipates SOPs for the use of all CM tools by Q4 FY 2023.
OIG Analysis:	The OIG inspected the DNFSB GSS Continuous Monitoring Policies and Procedures Guide and determined the use of the agency's continuous monitoring tools is documented. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 16:	Define the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program.
Agency Response Dated September 20, 2023:	DNFSB has updated documents supporting the ISCM program and will request closure of this recommendation.
OIG Analysis:	The OIG inspected the DNFSB GSS Continuous Monitoring Policies and Procedures Guide and noted that DNFSB has defined qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program in Appendix C: Continuous Monitoring Reports. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 17:	Define handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents.
Agency Response Dated September 20, 2023:	DNFSB updated its "Cyber Playbook v 1.5" document on 9/29/22 which lays out step-by-step response actions to take for different types of incidents, including identifying precursors for different event types. DNFSB will request closure of this recommendation.
OIG Analysis:	The OIG inspected the DNFSB Incident Response Process Guide Cyber Playbook and noted that DNFSB has defined handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 18:	Consistently test the incident response plan annually.
Agency Response Dated September 20, 2023:	DNFSB tested its incident response plan on 9/29/22. DNFSB provided evidence of this testing during the course of the audit. DNFSB will request closure of this recommendation. Note: This recommendation was rejected by OGM.
OIG Analysis:	DNFSB tested the incident response plan through a tabletop exercise on May 24-25, 2023, and produced evidence of lessons learned in the Hotwash section of the exercise report. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 19:	Update the Agency's incident response plan to reflect the US-CERT incident reporting guidelines.
Agency Response Dated September 20, 2023:	DNFSB requested this recommendation be closed in "CLOSURE OF FY21 AND FY22 FISMA AUDIT RECOMMENDATIONS" memo dated 8/19/22. Awaiting OIG validation as part of the FY23 FISMA Audit fieldwork.
OIG Analysis:	The OIG inspected the DNFSB Incident Response Plan and confirmed DNFSB's process for analyzing, documenting, and reporting security incidents is based on US-CERT guidelines. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 20:	Allocate and train staff with significant incident response responsibilities.
Agency Response Dated September 20, 2023:	DNFSB has identified appropriate Incident Response training and select members of the Incident Response Team have completed the training. DNFSB will deliver this training to identified individuals by Q1 FY 2024.
OIG Analysis:	The OIG will close this recommendation when the DNFSB allocates and trains staff with significant incident response responsibilities.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 21:	Configure all incident response tools in place to be interoperable, can collect and retain relevant and meaningful data that is consistent with the incident response policy, plans and procedures.
Agency Response Dated September 20, 2023:	DNFSB has deployed Microsoft Sentinel as its centralized Security Incident and Event Management (SIEM) tool. DNFSB will request closure of this recommendation.
OIG Analysis:	The OIG inspected the SIEM tool configuration and determined it is interoperable with other incident response tools in place. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(DNFSB-22-A-04)

Recommendation 22:	Develop and track metrics related to the performance of contingency planning and recovery related activities.
Agency Response Dated September 20, 2023:	DNFSB is currently revising the DNFSB GSS Information System Contingency Plan. An updated version with performance metrics is expected to be completed in Q4 FY 2023. DNFSB previously rejected this recommendation.
OIG Analysis:	The OIG will close this recommendation when the DNFSB documents in its guidance and/or directives metrics and a tracking mechanism related to the performance of contingency planning and recovery related activities.
Status:	Open: Resolved.

Recommendation 23:	Conduct a business impact assessment within every two years to assess mission essential functions and incorporate the results into strategy and mitigation planning activities.
Agency Response Dated September 20, 2023:	This recommendation will be resolved when an agency-wide BIA is performed. DNFSB will complete a BIA Q3 FY 2024.
OIG Analysis:	The OIG will close this recommendation when the DNFSB conducts a business impact assessment within every two years to assess mission essential functions and incorporate the results into strategy and mitigation planning activities.
Status:	Open: Resolved.

Recommendation 24:	Implement role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.
Agency Response Dated September 20, 2023:	DNFSB has identified appropriate contingency training and select members of the Contingency Planning Team have completed the training. DNFSB will deliver this training to identified individuals by Q1 FY 2024.
OIG Analysis:	The OIG will close this recommendation when the DNFSB implements role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.
Status:	Open: Resolved.