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 2020 (DNFSB-21-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 the recommendations as discussed in the agency's response dated September 20, 2023. Based on this response, recommendations 5, 6, 8, 12, and 13 have been closed, and recommendations 1 to 4, 7, 9 to 11, and 14 remain open and resolved. Please provide an updated status of the open and resolved 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 2020
Status of Recommendations
(DNFSB-21-A-04)

Recommendation 1:	Define an ISA in accordance with the Federal Enterprise Architecture Framework.
Agency Response Dated September 20, 2023:	DNFSB has completed development of our Zero Trust Implementation Plan and is actively working towards its implementation. This plan is the equivalent of an Information Security Architecture. Based on actions already taken, DNFSB's position is that this recommendation needs to be closed.
OIG Analysis:	A zero trust strategy is an important component of an Information Security Architecture; however, it focuses primarily on access control and network security. An ISA covers broader security areas, including governance, risk management, compliance, and various technical controls. This recommendation will be closed when the OIG verifies that the DNFSB has defined an ISA in accordance with the Federal Enterprise Architecture Framework.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(DNFSB-21-A-04)

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.

Agency Response Dated September 20, 2023:

a) DNFSB is currently contracting with an outside consultant to develop an Enterprise Risk Management (ERM) Program and process, which will assess risk at the enterprise level. DNFSB's existing Executive Committee on Internal Controls (ECIC) assesses risk at the business process level, and DNFSB's existing Risk Management Framework handbook, configuration management, and continuous monitoring processes assess risk at the information system level.

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.

c) DNFSB will conduct an organization wide security and privacy risk assessment once the ERM program has been established.

d) DNFSB will conduct a supply chain risk assessment in Q2 FY 2024.

Recommendation 2 (continued):

OIG Analysis:	This recommendation will be closed when the OIG verifies that the DNFSB's fully defined ISA is used in accordance with our recommendation.
Status:	Open: Resolved.

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 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 more effectively manage and optimize all domains of the DNFSB information security program; c. Implement a centralized view of risk across the organization; and, d. Implement formal procedures for prioritizing and tracking POA&M to remediate vulnerabilities.
Agency Response Dated September 20, 2023:	DNFSB is currently contracting with an outside consultant to develop an Enterprise Risk Management Program and a process in accordance with recommendation 2020-2. Once complete, DNFSB can begin working on this recommendation. a) DNFSB needs clarification from the OIG of the specific actions that are required to resolve this portion of the recommendation. b) DNFSB will review existing policies & procedures against the recommendations in NIST SP-800 55 Rev.2 and make any updates by Q2 FY 2024.

Recommendation 3 (continued):

c) DNFSB is currently contracting with an outside consultant to develop an Enterprise Risk Management (ERM) Program and process, which will assess risk at the enterprise level. DNFSB's existing Executive Committee on Internal Controls (ECIC) assesses risk at the business process level, and DNFSB's existing Risk Management Framework handbook, configuration management, and continuous monitoring processes assess risk at the information system level.

d) 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: This recommendation will be closed when the OIG verifies that the DNFSB fully completed all four elements in our recommendation. Subsection a) of this recommendation will require DNFSB to provide evidence of established performance metrics in service level agreements for the contractor systems and services monitored by IT Operations.

Status: Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(DNFSB-21-A-04)

Recommendation 4:	Finalize the implementation of a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in near real time. Continue ongoing efforts to apply the Track-It!, ForeScout, and KACE solutions.
Agency Response Dated September 20, 2023:	DNFSB has implemented Qualys, Intune, and Microsoft Defender as hardware/software monitoring platforms. These systems have dashboards, which provide a near real time view of hardware and software on the network. Track-It! and KACE have been implemented, and their configurations are refined as needed. Device compliance policies, enforced by Microsoft Intune, identify devices (agency laptops and iPhones) that are not running the current versions of Operating Systems. Only iPhones purchased through Apple Business Manager (formerly DEP) program can be enrolled in Intune, so no unauthorized mobile hardware can connect to DNFSB's IT resources (no BYOD devices allowed). Users cannot install unauthorized software (all software on iPhones must be approved and installed through Intune; users cannot access the Apple App Store). Based on actions already taken, DNFSB's position is that this recommendation needs to be closed.

Recommendation 4 (continued):

OIG Analysis:	The DNFSB did not provide evidence for detecting unauthorized hardware and its capability to deny access to agency enterprise services when security and operating system updates have not been applied for mobile devices based on agency policy or guidance within the given period. This recommendation will be closed when the OIG verifies that the DNFSB finalized the implementation of a centralized, automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in near real-time.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(DNFSB-21-A-04)

Recommendation 5:	Conduct remedial training to re-enforce requirements for documenting CCB's approvals and security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.
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 FISMA 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.

Recommendation 6:	Implement procedures and define roles for reviewing configuration change activities to the DNFSB's information system production environment by those with privileged access to verify the activity was approved by the system CCB and executed appropriately.
Agency Response Dated September 20, 2023:	DNFSB requested this recommendation be closed in "CLOSURE OF FY19 AND FY20 FISMA AUDIT RECOMMENDATIONS" memo dated 8/23/22. Awaiting OIG validation as part of the FY23 FISMA Audit fieldwork.
OIG Analysis:	The OIG inspected the DNFSB Configuration Management Policy and determined it documents roles/responsibilities for reviewing configuration change activities and stipulates approvals required for each requested change. Also, for a sample of ten changes from the population of 67 changes from October 1, 2022 to February 13, 2023, the OIG noted that all sampled changes were approved by the CCB and executed as appropriate in accordance with the DNFSB Configuration Management Policy. 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 2020
Status of Recommendations
(DNFSB-21-A-04)

Recommendation 7:	Implement a technical capability to restrict new employees and contractors from being granted access to the DNFSB's systems and information until a non-disclosure agreement is signed and uploaded to a centralized tracking system.
Agency Response Dated September 20, 2023:	DNFSB and the OIG have changed their processes and no longer require any users to sign a non-disclosure agreement in addition to the DNFSB IT User Agreement/Rules of Behavior form, which every user must sign prior to being granted access to DNFSB resources. DNFSB relies on documented procedures to ensure that users are not granted access to DNFSB information systems prior to completion of required training & signing of the IT User Agreement/Rules of Behavior form. DNFSB has created a new System Authorization Access Request (SAAR) process and automated workflow in SharePoint to streamline the new account creation process and is also in the process of acquiring an agency-wide automated ticketing solution, which will be used to more fully automate standard processes such as account provisioning/de-provisioning. When this new system is implemented, DNFSB will be able to close this recommendation. DNFSB plans to acquire this new ticketing system in Q4 2023 and put it into production by Q2 2024.

Recommendation 7 (continued):

OIG Analysis:	This recommendation will be closed when the OIG verifies that the DNFSB implemented a technical capability to restrict new employees and contractors from being granted access to the DNFSB's systems and information until documented procedures are performed and uploaded to a centralized tracking system.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(DNFSB-21-A-04)

Recommendation 8:	Implement the technical capability to require PIV or Identification and Authentication Level of Assurance (IAL) 3 to all DNFSB privileged accounts.
Agency Response Dated September 20, 2023:	DNFSB requested this recommendation be closed in "CLOSURE OF FY19 AND FY20 FISMA AUDIT RECOMMENDATIONS" memo dated 8/23/22. Awaiting OIG validation as part of the FY23 FISMA Audit fieldwork.
OIG Analysis:	The OIG inspected multifactor authentication configuration settings and determined that DNFSB has implemented strong authentication mechanisms to authenticate to applicable organizational systems and facilities, such as PIV and Windows Hello. 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 2020
Status of Recommendations
(DNFSB-21-A-04)

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.
Agency Response Dated September 20, 2023:	This is a duplicate of 2021-7. 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:	This recommendation will be closed when the OIG verifies that the DNFSB implemented 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.
Status:	Open: Resolved.

Recommendation 10:	Continue efforts to develop and implement role-based privacy training.
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; any additional privacy training will need to be coordinated with the Senior Agency Official for Privacy (SAOP).
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 2020
Status of Recommendations
(DNFSB-21-A-04)

Recommendation 11:	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. The exercises and after-action reports can be provided. 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 the DNFSB provide additional information pertaining to the testing of the breach response plan.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(DNFSB-21-A-04)

Recommendation 12:	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:	DNFSB published updates to the Risk Management Framework Handbook, which contains assessment procedures, and the Continuous Monitoring Policies and Procedures Guide, which refined monitoring requirements, in September 2022. 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 monitoring and assessment procedures and the updated authorization of the system. This recommendation is closed.
Status:	Closed.

Recommendation 13:	Update the DNFSB's incident response plan to include profiling techniques for identifying incidents and strategies to contain all types of major incidents.
Agency Response Dated September 20, 2023:	DNFSB updated its existing Incident Response Plan for the DNFSB GSS that reflects US-CERT incident reporting guidelines. A draft version of the updated document was provided to the FISMA auditors during their fieldwork in response to a PBC item request and a final version has been approved by the DNFSB CIO. During the course of the FY22 FISMA audit fieldwork, the auditors indicated that based on their review of the updated document, they consider this recommendation closed. DNFSB has also developed and continues to update a Cyber Playbook (currently at V. 1.5). A draft version of this document was provided to the FISMA auditors during their fieldwork in response to a PBC item request. The Cyber Playbook identifies the most likely types of cyberattacks and documents specific incident response procedures to follow to ensure consistent responses to security incidents. DNFSB updated the GSS Incident Response Plan on 9/13/22 and the Cyber Playbook on 9/29/22 and will request this recommendation be closed.
OIG Analysis:	The OIG inspected the DNFSB Incident Response Process Guide Cyber Playbook and determined it includes profiling techniques for incident identification and strategies for containing them. 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 2020
Status of Recommendations
(DNFSB-21-A-04)

Recommendation 14:	Based on the results of the DNFSB's supply chain risk assessment included in the recommendation for the Identify function above, update the DNFSB's contingency planning policies and procedures to address ICT supply chain risk.
Agency Response Dated September 20, 2023:	Recommendation is a duplicate of 2019-11. Supply Chain Risk, including ICT, will be addressed in an upcoming Supply Chain Risk Management Program Operating Procedure. The estimated completion is Q4 FY 2023.
OIG Analysis:	This recommendation will be closed when the OIG verifies that the DNFSB updated their contingency planning policies and procedures to address ICT supply chain risk, based on the DNFSB's supply chain risk assessment results included in the recommendation for the Identify function.
Status:	Open: Resolved.