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

REFERENCE: ASSOCIATE DIRECTOR FOR BOARD OPERATIONS, OFFICE OF THE CHIEF INFORMATION OFFICER MEMORANDUM 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 2 to 6, and 10 are closed, and recommendations 1 and 7 remain open and resolved. Recommendations 8, 9, and 11 were closed previously. 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
N. Thomas-Hawkins, OEDO

Audit Report
AUDIT OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2022
Status of Recommendations
(DNFSB-22-A-07)

Recommendation 1:	Implement a process to ensure a security control assessment for the DNFSB GSS is completed and documented on an annual basis.
Agency Response Dated September 20, 2023:	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, 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:	This recommendation will be closed when the OIG obtains and reviews the documented June 2023 and June 2024 external security assessments to verify the DNFSB has implemented a process to ensure a security control assessment for the DNFSB GSS is completed and documented annually.
Status:	Open: Resolved.

Audit Report
AUDIT OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2022
Status of Recommendations
(DNFSB-22-A-07)

Recommendation 2:	Implement a process to validate the DNFSB GSS security authorization is maintained in accordance with DNFSB policy.
Agency Response Dated September 20, 2023:	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, DNFSB completed an external security assessment in June of 2023 and issued an updated ATO for the DNFSB GSS in July 2023.
OIG Analysis:	The OIG reviewed the June 2023 documented external security assessment and July 2023 documented ATO, and determined it is maintained in accordance with DNFSB policy. This recommendation is closed.
Status:	Closed.

Audit Report
AUDIT OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2022
Status of Recommendations
(DNFSB-22-A-07)

Recommendation 3:	Enforce existing DNFSB policy requirements to document security impact analyses, test plans, test results and backout plan requirements for each change.
Agency Response Dated September 20, 2023:	DNFSB considers Recommendation 2022-3 to be fully remediated. DNFSB will request closure of this recommendation.
OIG Analysis:	The OIG reviewed a sample of ten changes from the population of 67 changes from October 1, 2022, to February 13, 2023, and no exceptions were found related to the enforcement of existing DNFSB policy requirements to document security impact analyses, test plans, test results, and backout plan requirements for each change as applicable. This recommendation is closed.
Status:	Closed.

Audit Report
AUDIT OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2022
Status of Recommendations
(DNFSB-22-A-07)

Recommendation 4:	Complete the implementation and consistent performance of monthly reviews to ensure security impact analyses, test plans, test results and backout plans are documented as required for each change.
Agency Response Dated September 20, 2023:	DNFSB has implemented a quarterly review of all change request tickets. DNFSB considers Recommendation 2022-4 to be fully remediated. DNFSB will request closure of this recommendation.
OIG Analysis:	Quarterly reviews were implemented in place of the recommended monthly reviews; however, the OIG verified that reviews to ensure change requirements are met were performed. This recommendation is closed.
Status:	Closed.

Recommendation 5:	Complete the implementation of the configuration management training program and provide periodic refreshers to ensure evidence requirements are captured for change tickets.
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. DNFSB published its "Security Awareness Training Policy" in August 2022 that contains requirements for role-based training and enforcement actions for individuals that do not complete required role-based training – this document was provided as a PBC item. 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 DNFSB provided documentation of the implementation of the configuration management training program and documentation of periodic refreshers to ensure evidence requirements are captured for change tickets. This recommendation is closed.
Status:	Closed.

Audit Report
AUDIT OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2022
Status of Recommendations
(DNFSB-22-A-07)

Recommendation 6:	Update the current change process, the Track-It! tool or both to enforce segregation of duties controls for a requestor and an approver of a change (e.g., requiring a second approver signature for all non-emergency changes, when the requester is eligible to be an approver).
Agency Response Dated September 20, 2023:	DNFSB considers Recommendation 2022-6 to be fully remediated. DNFSB will request closure of this recommendation.
OIG Analysis:	The OIG reviewed a sample of ten changes from the population of 67 changes from October 1, 2022, to February 13, 2023, and noted that all Track-It! tickets sampled required multiple configuration control board approvers (i.e., three) to vote to approve a change. This recommendation is closed.
Status:	Closed.

Recommendation 7:	Create procedures for vulnerability and compliance management based on risk and level of effort involved to mitigate confirmed vulnerabilities case-by-case such as: a. Prioritizing mitigation in accordance with all requirements specified by CISA BOD 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities and Emergency Directives, as applicable. b. Opening plans of action and milestones to track critical and high vulnerabilities that cannot be addressed within 30 days. c. Preparing risk-based decisions in unusual circumstances when there is a technical or cost limitation making mitigation of a critical or high vulnerability infeasible with documented, effective compensating controls coupled with a clear timeframe for planned remediation.
Agency Response Dated September 20, 2023:	DNFSB remediates vulnerabilities in accordance with OP-412.2-1: Vulnerability Management Operating Procedures. Any critical or high vulnerabilities that are not remediated within the timeframes defined in the OP are placed on a vulnerability POA&M. DNFSB is finalizing a standard template for risk acceptance actions when there is a technical or cost limitation making mitigation of a critical or high vulnerability infeasible with documented, effective compensating controls coupled with a clear timeframe for planned remediation. DNFSB will begin using the new risk acceptance template in FY 2024. DNFSB published OP 412.2-1, Vulnerability Management Operating Procedures, on 2/21/23. DNFSB considers Recommendation 2022-7 to be fully remediated. DNFSB will request closure of this recommendation.
OIG Analysis:	The OIG audit found the DNFSB does not remediate identified critical and high vulnerabilities in accordance with timeframes required by DNFSB policy. The OIG will close this recommendation when the DNFSB provides its procedures for vulnerability and compliance management,

Recommendation 7 (continued):

along with the finalized standard template for risk acceptance actions, and OIG determines it is based on risk and level of effort involved to mitigate confirmed vulnerabilities in the listed cases.

Status: Open: Resolved.

Audit Report
AUDIT OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2022
Status of Recommendations
(DNFSB-22-A-07)

Recommendation 10:	Document and implement system and information integrity and systems and communications protection policies and procedures in accordance with DNFSB policy.
Agency Response Dated September 20, 2023:	DNFSB published its System and Communications Protection Policy and its System and Information Integrity Policy, both on 11/29/22. DNFSB considers Recommendation 2022-10 to be fully remediated. DNFSB will request closure of this recommendation.
OIG Analysis:	The OIG inspected system and information integrity and systems and communications protection policies and noted that DNFSB documented and implemented them in accordance with DNFSB policy. This recommendation is closed.
Status:	Closed.