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 DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019 (DNFSB-20-A-05)

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 discussed in the agency's response dated September 20, 2023. Based on this response, recommendations 7, 9 and 10 have been closed, and recommendations 3, 5, 8, and 11 remain open and resolved. Recommendations 1, 2, 4, and 6 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

Recommendation 3: Using the results of recommendations one (1) and two (2) above:

a. Implement an automated solution to help maintain an up-to-date, complete, accurate, and readily available Agency-wide view of the security configurations for all its GSS components; Cybersecurity Team exports metrics and vulnerability reports and sends them to the CISO and CIO's Office monthly for review. Develop a centralized dashboard that Cybersecurity Team and the CISO can populate for real-time assessments of compliance and security policies.

b. Collaborate with DNFSB Cybersecurity Team Support to establish performance metrics in service level agreements to measure, report on, and monitor the risks related to contractor systems and services being monitored by Cybersecurity Team.

c. Establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program.

d. Implement a centralized view of risk across the organization.

Agency Response dated September 20, 2023:

a. DNFSB has implemented Qualys, Intune, and Defender as vulnerability and compliance management platforms. These systems have dashboards which provide an up-to-date, complete, accurate, and readily available agency wide view of security configurations. Vulnerability reports are provided to the CIO/CISO weekly and include the number of open vulnerabilities, the number of patches applied in the last 7 days, and detailed information on remediation efforts.

b. DNFSB needs clarification from the OIG of the specific actions that are required to resolve this portion of the recommendation.

Recommendation 3 (continued.):

c. DNFSB needs clarification from the OIG of the specific actions that are required to resolve this portion of the recommendation.

d. 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.

OIG Analysis: This recommendation will be closed when the DNFSB completes all four elements in Recommendation 3 and the OIG verifies completion. Subsection b) 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. Subsection c) of this recommendation will require DNFSB to utilize guidance from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, *Performance Measurement Guide for Information Security* to establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program.

Status: Open: Resolved.

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.
Agency Response Dated September 20, 2023:	The DNFSB Configuration Management Plan details change control procedures. Consequences for non-compliance are detailed in the DNFSB Configuration Management Policy, section 6: Compliance (revised March 2023), and the DNFSB Information Systems User Agreement + IT Equipment Agreement Form, section: Policy, Standards, and Procedures Must Be Followed. 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 reviewed the DNFSB Configuration Management Policy and the DNFSB GSS SSP security control implementation details for Configuration Management (CM) family controls and found the documents do not define consequences for not adhering to change control requirements, and do not reflect details about the conduct of remedial training as necessary for change control requirement reinforcement. DNFSB did provide evidence supporting the completion of configuration management training.
Status:	Open: Resolved.

Recommendation 7:	Complete and document a risk-based justification for not implementing an automated solution (e.g., Splunk) to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network.
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 evidence supporting the implementation of a suite of automated solutions and determined that a view of security configurations for information system components connected to DNFSB's network is now in place. This recommendation is closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019
Status of Recommendations
(DNFSB-20-A-05)

Recommendation 8:	Continue efforts to meet milestones of the DNFSB ICAM Strategy necessary for fully transitioning to DNFSB's "to-be" ICAM architecture.
Agency Response Dated September 20, 2023:	DNFSB continues to implement it's zero trust architecture, which encompasses the majority of DNFSB's "to-be" ICAM infrastructure. Without guidance on what specific additional actions the OIG feels need to taken, DNFSB cannot close out this recommendation.
OIG Analysis:	ICAM and zero trust are complementary components of an overall cybersecurity strategy; however, have different focus and principles. ICAM covers the managing and controlling of user entities, their credentials, and their access to resources within the network. Zero trust emphasizes strict access controls and continuous verification. This recommendation will be closed when the OIG verifies that the DNFSB continues to meet milestones necessary for transitioning to the DNFSB "to-be" ICAM architecture.
Status:	Open: Resolved.

Recommendation 9:	Complete 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 has refined the Continuous Monitoring Policies and Procedures Guide (March 2023) and the RMF Handbook (September 2022). Following the processes detailed in those documents, the DNFSB was able to grant an Authorization to Operate (ATO) for the DNFSB GSS. 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 reviewed the documentation of the external security assessment performed in June 2023 and the documented updated ATO for the DNFSB GSS in July 2023. This recommendation is closed.
Status:	Closed.

Recommendation 10:	Identify and fully define requirements for the incident response technologies DNFSB plans to utilize in the specified areas and how these technologies respond to detected threats (e.g., cross-site scripting, phishing attempts, etc.).
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 Incident Response Process Guide Cyber Playbook and determined requirements for incident response technologies are specified in conjunction with how they will be used to respond to detected threats. This recommendation is closed.
Status:	Closed.

Recommendation 11:	Based on the results of DNFSB's supply chain risk assessment included in the recommendation for the Identify function above, update DNFSB's contingency planning policies and procedures to address ICT supply chain risk.
Agency Response Dated September 20, 2023:	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 DNFSB addresses ICT supply chain risk in their contingency planning policies and procedures.
Status:	Open: Resolved.