November 18, 2021

MEMORANDUM TO: Joel C. Spangenberg
Executive Director of Operations

FROM: Eric Rivera **/RA/**
Acting Assistant Inspector General for Audit

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: GENERAL MANAGER, DEFENSE NUCLEAR FACILITIES SAFETY BOARD, CORRESPONDENCE DATED NOVEMBER 01, 2021

Attached is the Office of the Inspector General's (OIG) analysis and status of the recommendations discussed in the DNFSB's response dated November 01, 2021. Based on this response, recommendations three, five, and seven through 11 remain open and resolved. Recommendations one, two, four, and six were closed previously. Please provide an updated status of the open and resolved recommendations **by June 30, 2022.**

If you have any questions or concerns, please call me at (301) 415-5915 or Terri Cooper, Team Leader, at (301) 415-5965.

Attachment: As stated

cc: J. Biggins, GM
R. Howard

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

DNFSB-20-A-05

Status of Recommendations

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 November 01, 2021: Agree. The DNFSB continues to make progress in implementing its CDM Agency Dashboard, which will provide an up-to-date, complete, accurate, and readily available Agency-wide view of the security configurations for all its GSS components. The CDM Agency Dashboard will also provide part of a centralized dashboard that the Cybersecurity Team.

Recommendation 3 (cont'd):

and the CISO can populate for real-time assessments of compliance and security policies.

DNFSB needs to update internal policies and procedures to ensure that performance metrics in service level agreements for external systems are being monitored to measure, report on, and monitor the risks related to external systems and services being monitored by the Cybersecurity Team.

DNFSB needs to establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program. Performing the above tasks will allow DNFSB to implement a centralized view of risk across the organization.

Implementation of this recommendation is still in progress and is anticipated to be completed in 2nd quarter of FY 2023.

OIG Analysis: The proposed action meets the intent of the recommendation. The recommendation will be closed when the DNFSB fully completes all four elements in Recommendation three.

Status: Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

DNFSB-20-A-05

Status of Recommendations

Recommendation 5:	Management should re-enforce requirements for performing DNFSBs 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 November 01, 2021:	DNFSB has yet to identify the appropriate personnel to update the existing Configuration Management Plan to ensure that it contains change control procedures that accurately reflect the agency's current IT infrastructure and IT workforce and that it effectively balances the level of approval required with a change's potential impact. A corresponding review of the agency's internal ticketing tool and processes must be performed to ensure the requirements of the updated Configuration Management Plan can be implemented as automated workflows that can enforce required change control procedures while also not being unnecessarily burdensome for those that play a role in the change control process. Once the existing Change Management Plan has been updated and the corresponding changes have been implemented in the agency's ticketing system, general training in the change control ticketing process will have to be provided to all staff, and specialized role-based training will have to be provided to those who play a role in the change approval process. DNFSB anticipates completing this recommendation by 1st quarter FY 2023.

Recommendation 5 (cont'd):

OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies that DNFSB management has re-enforced requirements for performing 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.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

DNFSB-20-A-05

Status of Recommendations

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 November 01, 2021:	DNFSB no longer agrees that the agency should not implement an automated solution 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. DNFSB is in the process of implementing two automated solutions (the CDM Agency Dashboard and Microsoft Defender portal) that will provide this capability. DNFSB anticipates having both of these solutions implemented by 2nd quarter FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the DNFSB completes and documents 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 configuration for all information system components connected to the organization's network.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

DNFSB-20-A-05

Status of Recommendations

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 November 01, 2021:	DNFSB's ICAM strategy will be included in the wider Enterprise Architecture (EA) that the agency's new IT support contract has been tasked with creating by Q1 FY 2023. DNFSB anticipates completing this by 1st quarter FY 2023.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies that the DNFSB has continued efforts to meet milestones of the DNFSB ICAM strategy.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

DNFSB-20-A-05

Status of Recommendations

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 November 01, 2021:	DNFSB recognizes that existing procedures such as OP 411.2-1, Information Systems Security Program Certification and Accreditation Operating Systems, need to be revised to document an improved process that can support ongoing assessment. DNFSB anticipates completing this by 3rd quarter of FY 2023.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the DNFSB completes current efforts to refine existing monitoring and assessment procedures to support ongoing authorization of the DNFSB system more effectively.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

DNFSB-20-A-05

Status of Recommendations

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 November 01, 2021:	DNFSB will rely on the new IT support contractor (as opposed to a third-party contractor) to identify and fully define requirements for the incident response technologies DNFSB plans to use in specified areas, and how the technologies respond to detected threats. The new tools being implemented, such as the CDM Agency Dashboard (and the associated Qualys scanner) and additional Office 365 security features such as Microsoft Defender 365 will improve the agency's incident response capabilities. The agency also plans to leverage the Threat Attack Simulator tool in Office 365 to be able to develop internal phishing assessments. Additionally, the agency required all current users to complete additional Phishing Awareness training in FY21 and modified the new user on-boarding process to make all new users complete the Phishing Awareness training prior to being granted access. DNFSB anticipates fully completing this task by 3rd quarter of FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when

Recommendation 10 (cont'd):

the DNFSB identifies and fully defines requirements for the incident response technologies that the DNFSB plans to utilize in the

specified areas and how these technologies respond to detected threats.

Status: Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

DNFSB-20-A-05

Status of Recommendations

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 November 01, 2021:	The DNFSB will either utilize the new IT support contract or contract with a third-party contractor to perform a supply chain risk management assessment. Based on the results of the supply chain risk assessment, the agency will update internal contingency planning policies and procedures to address ICT supply risk chain. DNFSB anticipates fully completing this task by 1st quarter of FY 2023.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the DNFSB updates its contingency planning policies and procedures to address ICT supply chain risk based on the results of the DNFSB's supply chain risk assessment included in the recommendation for the Identify function.
Status:	Open: Resolved.