



March 31, 2022

MEMORANDUM TO: Joel C. Spangenberg
Executive Director of Operations

FROM: Eric Rivera */RA/*
Acting 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: GENERAL MANAGER, DEFENSE NUCLEAR FACILITIES
SAFETY BOARD, CORRESPONDENCE DATED
FEBRUARY 16, 2022

Attached is the Office of the Inspector General's (OIG) analysis and status of the recommendations discussed in the DNFSB's response dated February 16, 2022. Based on this response, recommendations 3, 5, and 7 through 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 August 31, 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

<u>Recommendation 3:</u>	Using the results of recommendations one (1) and two (2) above: <ol style="list-style-type: none">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.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.Establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program.Implement a centralized view of risk across the organization.
Agency Response dated February 16, 2022:	Implementation of this recommendation is still in progress and is anticipated to be completed in 4th quarter of FY2023.
OIG Analysis:	This recommendation will be closed when the DNFSB fully completes all four elements in Recommendation 3.
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

<u>Recommendation 5:</u>	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 February 16, 2022:	DNFSB will conduct training for all members and participants in the CCB's approvals and security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan. DNFSB anticipates completion of this recommendation by 1st quarter FY2024. DNFSB will update the Configuration Management Plan to define consequences for not following procedures. We anticipate completing this recommendation by 2nd quarter FY2024.
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
February 16, 2022: Implementation of this recommendation is still in progress and is anticipated to be completed in 1st quarter of FY2023.

OIG Analysis: This 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
February 16, 2022: Implementation of this recommendation is still in progress and is anticipated to be completed by 3rd quarter of FY2023.

OIG Analysis: This 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
February 16, 2022: DNFSB will complete current efforts to refine existing monitoring and assessment procedures. We anticipate completing this recommendation by 4th quarter FY2023.

OIG Analysis: This 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
February 16, 2022: Implementation of this recommendation is still in progress and is anticipated to be completed in 3rd quarter of FY2022.

OIG Analysis: This recommendation will be closed when 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
February 16, 2022: Implementation of this recommendation is still in progress and is anticipated to be completed by 4th quarter of FY2022.

OIG Analysis: This 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.