DEFENSE NUCLEAR FACILITIES SAFETY BOARD
WASHINGTON, D.C. 20004-2901

OFFICE OF THE INSPECTOR GENERAL

June 3, 2021

MEMORANDUM TO: James Biggins
General Manager

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 MAY 7, 2021

Attached is the Office of the Inspector General's (OIG) analysis and status of the recommendations discussed in DNFSB's response dated May 7, 2021. Based on this response, recommendations one, two, four, and six are closed, while recommendations three, five, and seven through 11 are open and resolved. Please provide an updated status of the open and resolved recommendations by October 15, 2021.

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: R. Howard, OGM

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 1:	Define an ISA in accordance with the Federal Enterprise Architecture Framework.
Initial Agency Response:	Agree. DNFSB will contract with a third-party contractor to define an ISA in accordance with the Federal Enterprise Architecture Framework. We anticipate completing this recommendation in 4th quarter of FY 2021.
Agency Response Dated May 7, 2021:	DNFSB is in the process of contracting with a third-party contractor to develop a Federal Enterprise Architecture Framework and define an ISA in accordance with the Federal Enterprise Architecture Framework. We anticipate providing an expected completion date for this recommendation in the quarterly update to the OIG.
OIG Analysis:	This recommendation will be closed and consolidated to Recommendation one in the Fiscal Year 2020 FISMA Report DNFSB-21-A-04.
Status:	Closed.

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 2:	Use the fully defined ISA to: a. Assess enterprise, business process, and information system level risk. b. Formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decision. c. Conduct an organization wide security and privacy risk assessment. d. Conduct a supply chain risk assessment.
Initial Agency Response:	Agree. To complete this recommendation, DNFSB will contract with a third-party contractor to use the fully defined ISA completed in Recommendation1. We anticipate completing this recommendation by 2nd quarter of FY 2022.
Agency Response Dated May 7, 2021:	To complete this recommendation, DNFSB is in the process of contracting with a third-party contractor to use the fully defined ISA completed in Recommendation 1 to complete Recommendation 2. We anticipate providing an expected completion date for this recommendation in the quarterly update to the OIG.
OIG Analysis:	This recommendation will be closed and consolidated to Recommendation two in the Fiscal Year 2020 FISMA Report DNFSB-21-A-04.
Status:	Closed.

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.

Initial Agency Response: Agree. DNFSB will use the results of completing Recommendations 1 and 2 above to complete the recommendation. We anticipate completing this recommendation in 2nd quarter FY2023.

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 (Continued)

Agency Response Dated May 7, 2021:	DNFSB will use the results of completing Recommendations 1 and 2 above to complete the recommendation. We anticipate providing an expected completion date for this recommendation in the quarterly update to the OIG.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when 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 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.
Initial Agency Response:	Agree. DNFSB will 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, and continue ongoing efforts to apply the Track-It!, ForeScout and KACE solutions. We anticipate completing this recommendation by 3rd quarter FY2021.
Agency Response Dated May 7, 2021:	DNFSB will finalize the implementation of a centralized automated solution for monitoring authorized and unauthorized hardware connected to the agency's network in near real time. DNFSB will investigate a solution for the implantation of a centralized automated solution for monitoring authorized and unauthorized software connected to the agency's network in near real time. We anticipate completing the hardware portion of this recommendation with ForeScout by 3rd quarter FY2021. DNFSB anticipates completing the investigation of a software solution by 4th quarter FY2021.
OIG Analysis:	This recommendation will be closed and consolidated to Recommendation four in the Fiscal Year 2020 FISMA Report DNFSB-21-A-04.
Status:	Closed.

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.
Initial Agency Response:	Agree. DNFSB will re-enforce requirements for performing change control procedures in accordance with the agency's Configuration Management Plan by defining consequences for not following procedures and conducting remedial training. We anticipate completing this recommendation by 2nd quarter FY2021.
Agency Response Dated May 7, 2021:	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 3rd quarter FY2021. DNFSB will update the Configuration Management Plan to define consequences for not following procedures. We anticipate completing this recommendation by 4th quarter FY2021.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when OIG verifies 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 6:	Implement procedures and define roles for reviewing configuration change activities to the DNFSB information system production environment by those with privileged access to verify the activity was approved by the system CCB and executed appropriately
Initial Agency Response:	Agree. DNFSB will implement procedures and define roles for reviewing configuration change activity to DNFSB's information system production environment by those with privileged access, to verify the activity was appropriately approved and executed. We anticipate completing this recommendation by 1st quarter FY2023.
Agency Response Dated May 7, 2021:	Implementation of this recommendation is still in progress and is anticipated to be completed by 1st quarter FY2023.
OIG Analysis:	This recommendation will be closed and consolidated to Recommendation six in the Fiscal Year 2020 FISMA Report DNFSB-21-A-04.
Status:	Closed.

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.
Initial Agency Response:	Agree. DNFSB will contract with a third-party contractor to complete and document a risk-based justification for not implementing an automated solution (e.g. Splunk) to help maintain security configurations for all information system components connected to the organization's network. We anticipate completing this recommendation by 2nd quarter FY 2022.
Agency Response Dated May 7, 2021:	Implementation of this recommendation is still in progress and is anticipated to be completed in 2nd quarter of FY2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when 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.
Initial Agency Response:	Agree. DNFSB will continue efforts to meet milestones of the DNFSB ICAM Strategy. We anticipate completing this recommendation by 1st quarter FY2023.
Agency Response Dated May 7, 2021:	Implementation of this recommendation is still in progress and is anticipated to be completed by the 1st quarter of FY 2023.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when OIG verifies that 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.
Initial Agency Response:	Agree. DNFSB will complete current efforts to refine existing monitoring and assessment procedures. We anticipate completing this recommendation by 3rd quarter FY2023.
Agency Response Dated May 7, 2021:	Implementation of this recommendation is still in progress and is anticipated to be completed in the 3rd quarter of FY 2023.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when 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.).
Initial Agency Response:	Agree. DNFSB will contract with 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. We anticipate completing this recommendation by 2nd quarter FY 2022.
Agency Response Dated May 7, 2021:	Implementation of this recommendation is still in progress and is anticipated to be completed in by the 2nd quarter of FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when DNFSB identifies and fully defines requirements for the incident response technologies 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.
Initial Agency Response:	Agree. DNFSB will contract with a third-party contractor to update DNFSB's contingency planning policies and procedures to address ICT supply risk chain, based on the results of DNFSB's supply chain risk assessment. We anticipate completing this recommendation by 3rd quarter FY 2022.
Agency Response Dated May 7, 2021:	Implementation of this recommendation is still in progress and is anticipated to be completed by the 3rd quarter of FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when DNFSB updates its contingency planning policies and procedures to address ICT supply chain risk based on the results of DNFSB's supply chain risk assessment included in the recommendation for the Identify function.
Status:	Open: Resolved.