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

OFFICE OF THE INSPECTOR GENERAL

June 4, 2021

MEMORANDUM TO: James Biggins
General Manager

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

SUBJECT: STATUS OF RECOMMENDATION: INDEPENDENT EVALUATION OF DNFSB'S IMPLEMENTATION OF FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 (DNFSB-21-A-04)

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 as discussed in DNFSB's response dated May 7, 2021. Based on this response, all recommendations (1 through 14) 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 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 1:	Define an ISA in accordance with the Federal Enterprise Architecture Framework.
Agency Response Dated May 7, 2021:	Agree. 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:	The proposed action meets the intent of the recommendation. This is a carryover recommendation from FY 2019 FISMA Evaluation (Report DNFSB-20-A-05). The recommendation will be closed when the OIG verifies that DNFSB has defined an ISA in accordance with the Federal Enterprise Architecture Framework.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 2: Use the fully defined ISA to:

a. Assess enterprise, business process, and information system level risks.

b. Formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.

c. Conduct an organization wide security and privacy risk assessment.

d. Conduct a supply chain risk assessment.

Agency Response Dated May 7, 2021: Agree. 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: The proposed action meets the intent of the recommendation. This is a carryover recommendation from FY 2019 FISMA Evaluation (Report DNFSB-20-A-05). The recommendation will be closed when the OIG verifies DNFSB's fully defined ISA and the ISA is used in accordance with our recommendation.

Status: Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 3:	Using the results of recommendations one (1) and two (2) above: a. Collaborate with the DNFSB's Cybersecurity Team 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 IT Operations; b. Utilize guidance from the National Institute of Standards in Technology (NIST) Special Publication (SP) 800-55 (Rev. 1) – Performance Measurement Guide for Information Security to establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program; c. Implement a centralized view of risk across the organization; and, d. Implement formal procedures for prioritizing and tracking POA&M to remediate vulnerabilities.
Agency Response Dated May 7, 2021:	Agree. 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 the OIG verifies 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 2020

DNFSB-21-A-04

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.
Agency Response Dated May 7, 2021:	Agree. 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:	The proposed action meets the intent of the recommendation. This is a carryover recommendation from FY 2019 FISMA Evaluation (Report DNFSB-20-A-05). The recommendation will be closed when the OIG verifies DNFSB finalize the implementation of a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in real time; and provides documentation of ongoing efforts to apply the Track-It! ForeScout and KACE solutions.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 5:	Conduct remedial training to re-enforce requirements for documenting CCB's approvals and security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.
Agency Response Dated May 7, 2021:	Agree. 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.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies DNFSB conducts remedial training to re-enforce requirements for documenting CCB's approvals and security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 6:	Implement procedures and define roles for reviewing configuration change activities to the DNFSB's information system production environment by those with privileged access to verify the activity was approved by the system CCB and executed appropriately.
Agency Response Dated May 7, 2021:	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.
OIG Analysis:	The proposed action meets the intent of the recommendation. This is a carryover recommendation from FY 2019 FISMA Evaluation (Report DNFSB-20-A-05). The recommendation will be closed when the OIG verifies DNFSB implement procedures and define roles for reviewing configuration change activities to DNFSB's information system production environment by those with privileged access to verify the activity was appropriately approved and executed.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 7:	Implement a technical capability to restrict new employees and contractors from being granted access to the DNFSB's systems and information until a non-disclosure agreement is signed and uploaded to a centralized tracking system.
Agency Response Dated May 7, 2021:	Agree. DNFSB will investigate a solution for the implementation of a technical capability to restrict new employees and contractors from being granted access to the DNFSB's systems and information until a non-disclosure agreement is signed and uploaded to a centralized tracking system.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when OIG verifies DNFSB implemented a technical capability to restrict new employees and contractors from being granted access to the DNFSB's systems and information until a non-disclosure agreement is signed and uploaded to a centralized tracking system
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 8:	Implement the technical capability to require PIV or Identification and Authentication Level of Assurance (IAL) 3 to all DNFSB privileged accounts.
Agency Response Dated May 7, 2021:	Agree. DNFSB will investigate a technical capability to implement the requirement for PIV or Identification and Authentication Level of Assurance (IAL) 3 to all DNFSB privileged accounts.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies DNFSB implemented the technical capability to require PIV or Identification and Authentication Level of Assurance (IAL) 3 to all DNFSB privileged accounts.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 9:	Implement automated mechanisms (e.g. machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.
Agency Response Dated May 7, 2021:	Agree. DNFSB will investigate an automated mechanism solution to implement to support the management or privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies DNFSB implemented automated mechanisms (e.g. machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 10:	Continue efforts to develop and implement role-based privacy training.
Agency Response Dated May 7, 2021:	Agree. DNFSB has hired a Director of Operational Services (DOS) who will be the Privacy Officer. The Privacy Officer will continue efforts to develop and implement role-based privacy training and provide a target date for completion in DNFSB's next scheduled update.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies DNFSB is continuing efforts to develop and implement role-based privacy training.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 11:	Conduct the agency's annual breach response plan exercise for FY 2021.
Agency Response Dated May 7, 2021:	Agree. DNFSB will conduct an annual breach response plan exercise for FY2021. DNFSB anticipates completion of this recommendation by 4th quarter FY2021.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies DNFSB conducted the agency's annual breach response plan exercise for FY 2021.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 12:	Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.
Agency Response Dated May 7, 2021:	Agree. DNFSB will complete current efforts to refine existing monitoring and assessment procedures. We anticipate completing this recommendation by 3rd quarter FY2023.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies DNFSB continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 13:	Update the DNFSB's incident response plan to include profiling techniques for identifying incidents and strategies to contain all types of major incidents.
Agency Response Dated May 7, 2021:	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 FY2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies DNFSB update the DNFSB's incident response plan to include profiling techniques for identifying incidents and strategies to contain all types of major incidents.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 14:	Based on the results of the DNFSB's supply chain risk assessment included in the recommendation for the Identify function above, update the DNFSB's contingency planning policies and procedures to address ICT supply chain risk.
Agency Response Dated May 7, 2021:	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 FY2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies DNFSB update the DNFSB's 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.