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 2020 (DNFSB-21-A-04)

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 as discussed in the DNFSB's response dated November 01, 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, **June 15, 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 2020

DNFSB-21-A-04

Status of Recommendations

Recommendation 1:	Define an ISA in accordance with the Federal Enterprise Architecture Framework.
Agency Response Dated November 01, 2021:	Agree. The DNFSB awarded a new IT support contractor in September 2021, and the performance work statement (PWS) for this contract includes a requirement for the contractor to "develop an Information Enterprise Architecture (EA) Program using the Federal Enterprise Architecture (FEA) reference models to standardize and improve IT management processes across the agency." Developing this EA is a prerequisite for developing the Information Security Architecture (ISA) that will satisfy this recommendation. DNFSB anticipates developing its EA by 1st quarter of FY 2023 and developing the related ISA by 3rd quarter of FY 2023.
OIG Analysis:	The proposed action meets the intent of the recommendation. This is a carryover recommendation from the FY 2019 FISMA Evaluation (Report DNFSB-20-A-05). The recommendation will be closed when the OIG verifies that the 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 November 01, 2021: Agree. The DNFSB intends to leverage its new IT support contract to develop its ISA by 3rd quarter of FY 2023 and anticipates being able to formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions by 1st quarter FY 2024 (Recommendation 2b).

DNFSB will be able assess enterprise, business process, and information system level risks and conduct an organization wide security and privacy risk assessment in parallel with the development of the ISA, as it will be an assessment of the "As Is" of the organization's security and privacy risk. DNFSB anticipates completing these tasks by 4th quarter FY 2024 (Recommendation 2a & 2c).

Recommendation 2 (cont'd):

Evaluation Report

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

DNFSB-21-A-04

	Status of Recommendations 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 (Recommendation 2d).
OIG Analysis:	The proposed action meets the intent of the recommendation. This is a carryover recommendation from the FY 2019 FISMA Evaluation (Report DNFSB-20-A-05). The recommendation will be closed when the OIG verifies that the DNFSB's fully defined 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 November 01, 2021:

Agree. DNFSB will review the established service level agreements (SLA) and continuous monitoring metrics provided by all of the FedRAMP cloud service providers (CSP) leveraged by the DNFSB to ensure SLA are being met and risks related to the use of external CSPs are being monitored. The DNFSB anticipates completing this task by Q3 FY 2022 (Recommendation 3a).

DNFSB will 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

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 (cont'd):

DNFSB information security program. DNFSB anticipates completing this task by Q4 FY 2022 (Recommendation 3b).

DNFSB has already started implementing a centralized view of risk across the organization that focuses on the DNFSB GSS (internal network) and the Office 365 GCC. DNFSB anticipates including all other external systems and completing this task by Q3 FY 2022 (Recommendation 3c).

DNFSB will implement formal procedures for prioritizing and tracking POA&M to remediate vulnerabilities in all information systems leveraged by the DNFSB. DNFSB anticipates including all other external systems and completing this task by Q3 FY 2022 (Recommendation 3d).

OIG Analysis: The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies that 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 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 November 01, 2021:	Agree. The DNFSB is implementing a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in near real time. The solution will leverage data from the CDM Agency Dashboard, Defender for Microsoft 365, and the agency's ForeScout CounterAct appliance. DNFSB anticipates completing this task by Q3 FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. This is a carryover recommendation from the FY 2019 FISMA Evaluation (Report DNFSB-20-A-05). The recommendation will be closed when the OIG verifies that the DNFSB finalizes 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 November 01, 2021:	Agree. DNFSB has yet to identify the appropriate personnel to review and 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 the DNFSB conducted 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 November 01, 2021:	Agree. DNFSB has to identify the appropriate personnel to review and 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 task by 1st quarter FY 2023.

Recommendation 6 (cont'd)

OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation is a carryover from the FY 2019 FISMA Evaluation (Report DNFSB-20-A-05). The recommendation will be closed when the OIG verifies that the DNFSB implemented procedures and defined roles for reviewing configuration change activities to the 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 November 01, 2021:	Agree. One of the tasks identified for completion by the DNFSB's new IT support contractor is the creation of automated workflows for onboarding and offboarding of employees and contractors. The goal of this task is to automate the process of submitting the initial requests for accounts and IT equipment for new users, tracking of the completion of all required training, the submission of all required forms, and the resulting creation of approved accounts and issuance of IT equipment. For offboarding, the goal is to automate the process of submitting requests for termination of access, verifying assigned IT equipment has been returned, and verifying all accounts have been disabled and eventually deleted. DNFSB anticipates completing this task by 3rd quarter FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies that the 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 November 01, 2021:	Agree. All DNFSB users already must authenticate with a PIV credential prior to accessing any privileged accounts on the DNFSB GSS (internal network), and all DNFSB users must already authenticate with a PIV credential to their local workstation and then authenticate using Microsoft Multi Factor Authentication (MFA) via the Microsoft Authenticator app, which is a NIST Authentication Assurance Level (AAL) 2 authenticator. Since GSA will not issue two PIV credentials to the same person (a normal user and the same person when performing a privileged role), the DNFSB is investigating alternative solutions that provide an equivalent level of identity assurance when privileged users access the agency's Office 365 tenant. Technical solutions being investigated include derived credentials (PIV-I), Microsoft's "PIV Native" offering (not currently approved for use in the Office 365 Government Community Cloud), or other Microsoft authentication options, such as using Windows Hello for Business (facial recognition) + TPM hardware or using FIDO2 security keys (USB security tokens); both of these solutions are NIST Authentication Assurance Level (AAL) 3 authenticators. For other systems outside of the DNFSB GSS and Office 365 GCC, DNFSB is working to ensure all external systems support Multi Factor Authentication (MFA) as required by

Recommendation 8 (cont'd):

Executive Order 14028. Many of the external systems leveraged by DNFSB, such as eOPF, the CDM Agency Dashboard, and DHS CyberScope already leverage PIV authentication provided by the OMB MAX portal.

DNFSB anticipates completing this task 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 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 November 01, 2021:	Agree. For Office 365 GCC, the DNFSB has begun using Microsoft's Privileged Identity Manager (PIM) tool, which requires users (with two fail-safe exceptions) to request permission whenever they need to elevate to a privileged role, which then grants them access for an 8-hour period, after which they have to request permission again. Role assignments for users with a fixed duration (such as for contractors working on a contract with a fixed duration) can be configured to have their access to privileged roles automatically deleted on a given date, such as the end date of the contract. For the DNFSB GSS, the agency uses the Varonis tool to generate reports on expiring, disabled and inactive accounts, and currently relies on manual disabling and removing of accounts and is investigating ways to automate the process as part of the automated workflow for offboarding discussed in Recommendation 7 above. DNFSB anticipates completing this task by 3rd quarter FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies that the DNFSB implemented automated mechanisms (e.g., machine-based, or user-based

Recommendation 9 (cont'd):

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 November 01, 2021:	Agree. DNFSB anticipates completing this task 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 continues developing and implementing 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 November 01, 2021:	Agree. DNFSB is holding a Cyber COOP exercise on November 17, 2021 that includes an inject that will serve as an annual breach response exercise.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies that the 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 November 01, 2021:	Agree. DNFSB is revising its internal procedures for ongoing authorization in support of granted Authorities to Operate (ATOs). DNFSB anticipates completing this task by 3rd quarter FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies that the DNFSB is continuing 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 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 November 01, 2021:	Agree. DNFSB will rely on the new IT support contractor (as opposed to a third-party contractor) to fully define requirements for the incident response technologies DNFSB plans to use in specified areas, and how the technologies respond to detected threats. DNFSB anticipates fully completing this task by 4th quarter of FY 2022.
OIG Analysis:	The proposed action meets the intent of the recommendation. The recommendation will be closed when the OIG verifies that the DNFSB updates the agency'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 November 01, 2021:	Agree. 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 OIG verifies that the DNFSB updates their contingency planning policies and procedures to address ICT supply chain risk, based on the DNFSB's supply chain risk assessment results included in the recommendation for the Identify function.
Status:	Open: Resolved.