May 3, 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 THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021 (DNFSB-22-A-04)

REFERENCE: OFFICE OF THE GENERAL MANAGER, MEMORANDUM DATED JANUARY 25, 2022; OFFICE OF THE EXECUTIVE DIRECTOR OF OPERATIONS, EMAIL DATED FEBRUARY 16, 2022

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency responses dated January 25, 2022, and February 16, 2022. Based on these responses, recommendation 18 (recommendation 13 in DNFSB's response) is considered open and unresolved. All other recommendations are open and resolved. Please provide an updated status of all 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: T. Tadlock, OEDO
R. Howard, OEDO

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 1:	Update the ISA and use the updated ISA to: a. Assess enterprise, business process, and information system level risks; b. Update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.
Agency Response Dated February 16, 2022:	Agree. We anticipate to provide the recommendation to the OIG by 1st quarter of FY 2023.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates the Information Security Architecture (ISA) to assess risk and update risk tolerance and appetite levels necessary for prioritizing and guiding risk management on the enterprise, business process, and information system levels.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 2:	Using the results of recommendations one above: a. Utilizing 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 manage and optimize all domains of the DNFSB information security program more effectively; b. Implement a centralized view of risk across the organization; c. Implement formal procedures for prioritizing and tracking POA&Ms to remediate vulnerabilities.
Agency Response Dated February 16, 2022:	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 OIG will close this recommendation when the DNFSB updates the ISA to utilize guidance form NIST to establish metrics to manage and optimize all domains of the DNFSB information security program more effectively; implement a centralized view of risk across the organization; and, implement formal procedures for prioritizing and tracking plan of actions and milestones (POA&Ms) to remediate vulnerabilities.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 3:	Update the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, to include: a. Defining a frequency for conducting Risk Assessments to periodically assess agency risks to integrate results of the assessment to improve upon mission and business processes.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a corrective action plan (CAP) for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, including defining a frequency for conducting risk assessments to periodically assess agency risks to integrate results of the assessment to improve upon mission and business processes.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 4:	Define a Supply Chain Risk Management strategy to drive the development and implementation of policies and procedures for: a. How supply chain risks are to be managed across the agency; b. How monitoring of external providers compliance with defined cybersecurity and supply chain requirements; c. How counterfeit components are prevented from entering the DNFSB supply chain.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB defines a supply chain risk management strategy to drive the development and implementation of policies and procedures for the items in bullets a. through c. above.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 5:	Conduct remedial training to re-enforce requirements for documenting security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB conducts remedial training to re-enforce requirements for documenting 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 DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 6:	Integrate the Configuration management plan with risk management and continuous monitoring programs and utilize lessons learned to make improvements to this plan.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB integrates the configuration management plan with risk management and continuous monitoring programs and utilizes lessons learned to make improvements to this plan.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 7:	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 February 16, 2022:	Agree. DNFSB will conduct market research on 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 OIG will close this recommendation when the DNFSB implements automated mechanisms 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 DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 8:	Continue efforts to implement data loss prevention functionality for the Microsoft Office 365 environment.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB continues its efforts to implement data loss prevention functionality for the Microsoft Office 365 environment.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 9:	Update agency strategic planning documents to include clear milestones for implementing strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates agency strategic planning documents to include clear milestones for implementing strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 10:	Conduct the agency's annual breach response plan exercise for FY 2021.
Agency Response Dated February 16, 2022:	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 OIG will close this recommendation when the DNFSB provides documentation that they conducted the agency's annual breach response plan exercise for FY 2021.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 11:	Continue efforts to develop and implement role-based privacy training for users with significant privacy or data protection related duties.
Agency Response Dated February 16, 2022:	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 OIG will close this recommendation when the DNFSB continues efforts to develop and implement role-based privacy training for users with significant privacy or data protection related duties.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 12:	Formally document requirements and procedures for the completion of role-based training and enforcement methods in place for individuals who do not complete role-based training.
Agency Response Dated January 25, 2022:	Disagree. The auditors failed to credit the agency with its 100 percent completion rate of role-based training. No corrective action is necessary.
OIG Analysis:	Based on subsequent discussions with the Executive Director of Operations (EDO) and documentation provided by the DNFSB, this recommendation is open and resolved. The OIG will close this recommendation when the DNFSB formally documents in DNFSB guidance and/or directives the requirements and procedures for the completion of role-based training and enforcement methods in place for individuals who do not complete the role-based training.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 13:	Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB continues 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 DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 14:	Update the DNFSB ISCM policies and procedures clearly defining what needs to be monitored at the system and organization level.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates its DNFSB ISCM policies and procedures clearly defining what needs to be monitored at the system and organization levels.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 15:	Define standard operating procedures for the use of the agency's continuous monitoring tools or update the continuous monitoring plan to include the use of new monitoring tools.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB defines standard operating procedures for the use of the agency's continuous monitoring tools or updates the continuous monitoring plan to include the use of new monitoring tools.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 16:	Define the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB defines the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 17:	Define handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB defines handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents.
Status:	Open: Resolved.

Status of Recommendations

Recommendation 18:	Consistently test the incident response plan annually.
Agency Response Dated January 25, 2022:	Disagree. The auditors failed to credit the DNFSB with the incident testing it performed. The agency tests its incident response through review of significant cyber incidents at other Federal agencies and in conjunction with its COOP exercises. No corrective actions are needed.
OIG Analysis:	OIG reviewed the information provided by the DNFSB and determined that it does not meet the intent of this recommendation. There was no evidence of a review of significant cyber incidents at other Federal agencies, and out of the eight after action reports provided, only the one titled "After Action Report COOP and IT Cybersecurity Exercise 17 Nov 2021", mentions incident response. Under "Areas for Improvement, Operational Support" it states, "Other than references to the COOP plan, ERG did not mention or refer to any other internal policies such as the IT Incident Response Plan, IT Disaster Recovery Plan, or Privacy Act Breach Response Plan." Under "Areas Identified for Further Discussion" Inject #4 states "The IT staff mentioned referring to the DNFSB COOP plan and IT Incident Response Plan but did not simulate following any of the steps in either plan as part of the exercise." Inject #5 states "The IT staff did not simulate following the steps outlined in either the IT Incident Response Plan or the IT Disaster Recovery Plan."

Recommendation 18 (cont.):

Under "General Observations" it provides "For incidents where core services (power, Internet connectivity) are not disrupted at the DNFSB HQ location, the COOP site provides little to no added value in incident response."

The OIG will move this recommendation to open and resolved when the DNFSB states in writing that it will test the incident response plan annually. The OIG will close this recommendation when DNFSB begins testing the incident response plan annually.

Status: Open: Unresolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 19:	Update the Agency's incident response plan to reflect the USCERT incident reporting guidelines.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB updates the agency's incident response plan to reflect the USCERT incident reporting guidelines.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 20:	Allocate and train staff with significant incident response responsibilities.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB allocates and trains staff with significant incident response responsibilities.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 21:	Configure all incident response tools in place to be interoperable, can collect and retain relevant and meaningful data that is consistent with the incident response policy, plans and procedures.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB configures all incident response tools in place to be interoperable, can collect and retain relevant and meaningful data that is consistent with the incident response policy, plans and procedures.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 22:	Develop and track metrics related to the performance of contingency planning and recovery related activities.
Agency Response Dated January 25, 2022:	Disagree. The auditors failed to identify disaster recovery events that required tracking of metrics. If events occur, DNFSB will report and track those events. No corrective action is needed.
OIG Analysis:	Based on subsequent discussions with the EDO, and DNFSB acknowledgment that it will consider the best process to develop and track metrics for the performance of contingency planning and recovery related activities, this recommendation is open and resolved. The OIG will close this recommendation when the DNFSB documents in its guidance and/or directives metrics and a tracking mechanism related to the performance of contingency planning and recovery related activities.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 23:	Conduct a business impact assessment within every two years to assess mission essential functions and incorporate the results into strategy and mitigation planning activities.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB conducts a business impact assessment within every two years to assess mission essential functions and incorporate the results into strategy and mitigation planning activities.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

DNFSB-22-A-04

Status of Recommendations

Recommendation 24:	Implement role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.
Agency Response Dated January 25, 2022:	Agree. DNFSB will provide a CAP for this recommendation in conjunction with existing FISMA recommendations in its consolidated update in February 2022.
OIG Analysis:	The OIG will close this recommendation when the DNFSB implements role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.
Status:	Open: Resolved.