MEMORANDUM

DATE: March 31, 2025

TO: Mary J. Buhler
Executive Director of Operations

FROM: Hruta Virkar, CPA */RA/*
Assistant Inspector General for Audits & Evaluations

SUBJECT: STATUS OF RECOMMENDATIONS: AUDIT OF THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023 (DNFSB-23-A-04)

REFERENCE: OFFICE OF THE EXECUTIVE DIRECTOR OF OPERATIONS, MEETING DATED FEBRUARY 26, 2025, AND EMAIL CORRESPONDENCE DATED FEBRUARY 27, 2025

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations, as discussed in a meeting between the OIG and the Defense Nuclear Facilities Safety Board (DNFSB) on February 26, 2025, and the DNFSB's email correspondence dated February 27, 2025. Based on this response, recommendation 1 remains open and resolved. Please provide an updated status of the open, resolved recommendation by July 11, 2025.

If you have any questions or concerns, please call me at 301.415.1982 or Mike Blair, Team Leader, at 301.415.8399.

Attachment:
As stated

cc: K. Herrera, DEDO
J. Biggins, DEDRS
G. Garvin, DEDRS

Audit Report
AUDIT OF THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023
Status of Recommendations
(DNFSB-23-A-04)

Recommendation 1:	We recommend that DNFSB's Chief Information Security Officer acquires resources to adequately support the procurement, onboarding, and implementation of requirements across all event logging maturity tiers to ensure events are logged and tracked in accordance with Office of Management and Budget (OMB) Memorandum (M)-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (August 27, 2021).
Agency Response Dated February 27, 2025:	DNFSB is now capturing all required logs for Criticality Levels 1, 2, & 3 as required by OMB M-21-31. The Logging Requirements M-21-31.xlsx file lists all of the required log types and a mapping to the specific logs that are being captured along with the log location. NOTE: a hands-on walkthrough of the various playbooks in the Sentinel Security Information and Event Management (SIEM) would be helpful to demonstrate how the logs are being captured & accessed.
OIG Analysis:	After reviewing the evidence, the OIG has concluded that additional artifacts are needed, such as screenshots of the various playbooks in Sentinel SIEM, to demonstrate how logs are being captured and accessed. Therefore, this recommendation remains open and resolved. The OIG will verify if corrective actions have been taken by the DNFSB to address this recommendation during its FY25 Federal Information Security Modernization Act of 2014 audit.
Status:	Open: Resolved