Defense Nuclear Facilities Safety Board
Washington, DC 20004-2901

Office of the Inspector General

July 15, 2015

MEMORANDUM TO: Mark T. Welch
General Manager

FROM: Stephen D. Dingbaum ***/RA/***
Assistant Inspector General for Audits

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014 (DNFSB-15-A-02)

REFERENCE: GENERAL MANAGER, DEFENSE NUCLEAR FACILITIES SAFETY BOARD, CORRESPONDENCE DATED JULY 1, 2015

Attached is the Office of the Inspector General's analysis and status of recommendations as discussed in the Board's response dated July 1, 2015. Based on this response, all recommendations remain resolved. Please provide an updated status of the resolved recommendations by November 30, 2015.

If you have any questions or concerns, please call me at 415-5915 or Beth Serepca, Team Leader, at 415-5911.

Attachment: As stated

CC: R. Howard, OGM

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 1: Perform an annual security control assessment of the General Support System (GSS). Since the Board has not identified the process for identifying which subset of controls should be tested each year, for FY 2015, OIG recommends the following controls should be tested at a minimum:

- Any controls that are new or changed in NIST SP 800-53 Revision 4.
- Any security control enhancements not tested during the 2012 security assessment.
- Any controls impacted by changes to the GSS environment since the security assessment conducted in 2012.
- Any controls associated with the closed Plan of Action and Milestones (POA&M) items.

Agency Response Dated July 1, 2015: We now expect to complete annual security controls testing by the end of the 4th Quarter FY 2015, due to the longer than expected time needed to update the SSP for the Board's GSS LAN, to include SP 800-53 Rev. 4 controls.

OIG Analysis: The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the security assessment was and will continue to be conducted to include the four specific steps as detailed in the recommendation.

Status: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 2:	Update the GSS security authorization documentation (e.g., Security Plan, Risk Assessment and the Security Assessment Report) as required.
Agency Response Dated July 1, 2015:	Implementation of this recommendation is in process. Updates to the security authorization handbook, is currently in the formal Green Folder review process. We expect to complete the process of updating all security authorization documentation no later than the 4th Quarter FY 2015.
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives the verification that the GSS security authorization documentation has been updated.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 3:	Reevaluate the risk assigned to the controls impacted by the error in the 2012 GSS risk assessment and update the POA&M as needed.
Agency Response Dated July 1, 2015:	The Board plans to test all of the GSS LAN's security controls and re-evaluate risk to the system based on the results of the new security control testing, in lieu of re-evaluating the risk assigned to all controls from the 2012 risk assessment. This approach will provide a more accurate assessment of the risks the system faces than the testing performed in 2012. We anticipate completion by 4th Quarter FY 2015.
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the risk assigned to the controls impacted by the error were reevaluated and the POA&M was updated as needed.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 4:	Update the GSS System Security Plan to document risk.
Agency Response Dated July 1, 2015:	Implementation of this recommendation is in process. Both the System Security Plan (SSP) and the System Characterization Document (SCD) for the GSS LAN are currently being updated. We expect to complete the update of the GSS System Security Plan no later than the 4th Quarter FY 2015.
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the GSS System Security Plan was updated to document risk.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 5:	Develop, document, and implement POA&M management procedures.
Agency Response Dated July 1, 2015:	Implementation of this recommendation is in process. An update to OP 411.2-1 that includes the new Security Authorization Handbook as an Appendix is currently in the formal Green Folder review process. We expect to complete implementation of new the new POA&M procedures by the end of the 4th Quarter 2015.
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that POA&M management procedures were developed, documented, and implemented.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 6:	Update the POA&M to include all known vulnerabilities and actual completion dates for the completed POA&M activities.
Agency Response Dated July 1, 2015:	The current plan is to develop a new list POA&M items based on the results of the testing of all of the GSS LAN's security controls. Any items from the existing POA&M list that are no longer valid based on the results of the new testing will be closed out. We expect to complete the update of the POA&M in the 4th Quarter FY 2015.
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the POA&M has been updated to include all known vulnerabilities and actual completion dates for the completed POA&M activities.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 7:	Develop, document, and implement procedures for performing oversight of systems operated by contractors and other Federal agencies.
Agency Response Dated July 1, 2015:	Implementation of this recommendation is in process. This finding will be partially satisfied by the publication of the updated OP 411.2-1 and associated new Security Authorization Handbook. We expect to complete the implementation of new oversight procedures for external systems no later than the 4th Quarter FY 2015.
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that procedures for performing oversight of systems operated by contractors and other Federal agencies have been developed, documented, and implemented.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 8:	As a best practice, for federally operated systems, in addition to obtaining ATOs for those systems, also request confirmation of annual contingency plan testing and annual security control testing for those systems.
Agency Response Dated July 1, 2015:	Implementation of this recommendation is in process. This finding will initially be addressed by the publication of a new Board Notice that has been submitted for formal review. We expect to implement the process for requesting more detailed ATO memos by the end of 4th Quarter FY 2015.
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the Board has received the required ATOs and confirmation that annual contingency plan testing and annual security control testing was performed for the federally operated systems.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014

DNFSB-15-A-02

Status of Recommendations

Recommendation 9:	Develop a plan and schedule for authorizing contractor-operated systems, including cloud-based systems, in accordance with FISMA, the NIST RMF, and FedRAMP.
Agency Response Dated July 1, 2015:	Implementation of this recommendation is in process. The Board is in the process of determining the most effective way to authorize contractor systems, especially cloud-based systems that are not currently in the process of FedRAMP certification or have already received a FedRAMP certification. We expect to complete authorizing all contractor-operated systems no later than 4th Quarter FY 2015.
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the Board has developed a plan and schedule for authorizing contractor-operated systems as detailed above.
Status:	Resolved.