Defense Nuclear Facilities
Safety Board
Washington, DC 20004-2901

Office of the
Inspector General

December 18, 2014

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 DECEMBER 12, 2014

Attached is the Office of the Inspector General's analysis and status of recommendations as discussed in the Board's response dated December 12, 2014. Based on this response, all recommendations are resolved. Please provide an updated status of the resolved recommendations by July 1, 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

Audit 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 December 12, 2014: Agree. The DNFSB agrees that it needs to perform an annual security control assessment of the GSS in FY 2015. The DNFSB will ensure that this security control assessment, performed by an external security assessor, addresses not only the four specific steps identified above but also tests all of the controls impacted by errors in the risk assessment performed in 2012 that are identified in Recommendation 3, below. We expect to complete annual security controls testing by the end of the 3rd 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 security assessment was and will continue to be conducted to include the four specific steps as detailed in the recommendation.

Status: Resolved.

Audit 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 December 12, 2014: Agree. The DNFSB agrees that in conjunction with a new annual security control assessment for the GSS, all related security authorization documentation will be updated. At a minimum, the DNFSB agrees to update the System Characterization Document, the System Security Plan, the Risk Assessment, and the Security Assessment Report for the GSS to ensure that an accurate picture of the current state of the GSS and the implementation of security controls is documented in support of ongoing authorization decisions. 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.

Audit 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

<u>Recommendation 3:</u> 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 December 12, 2014: Agree. The DNFSB agrees to re-evaluate the risk assigned to all of the controls that were impacted by errors made in the 2012 GSS *Risk Assessment* and update the existing POA&M as needed. In addition, as discussed in the response to Recommendation 1, the DNFSB agrees to make sure all of the controls that were impacted by errors made in the 2012 GSS risk assessment are included in the annual security control assessment of the GSS performed in FY 2015. We expect to complete the re-evaluation of risk by the end of 3rd 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.

Audit 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 December 12, 2014: Agree. The DNFSB agrees to update the *System Security Plan* to document accepted risk. Any risks that are identified in the annual security control assessment of the GSS performed in FY 2015 and recommended to be accepted will be documented in the *System Security Plan* for the GSS to ensure adequate documentation of the DNFSB's acceptance of any residual risk. 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.

Audit 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 December 12, 2014: Agree. The DNFSB agrees to develop, document and implement POA&M management procedures. The current procedures, "OP 411.2-1, Certification and Accreditation Operating *Procedures,"* will be replaced by a comprehensive *Security Authorization Handbook* that will include the POA&M management procedures and will assist the Board in implementing continuous monitoring in support of ongoing authorizations of the GSS. We expect to complete implementation of new the POA&M procedures by the end of the 3rd Quarter FY 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.

Audit 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 December 12, 2014: Agree. The DNFSB agrees to update the POA&M to include all known vulnerabilities and actual completion dates for the completed POA&M items. As mentioned earlier in the response to Recommendation 1, the DNFSB also agrees to test all security controls associated with the closed POA&M items in FY 2015 to ensure that the remediations previously performed on the closed POA&M items remain effective. 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.

Audit 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
December 12, 2014: Agree. The DNFSB agrees to develop, document, and implement procedures for performing oversight of external systems that are operated by contractors or other Federal agencies. For those systems that are contractor operated and also cloud-based, the DNFSB will leverage FedRAMP when possible. For those systems that are operated by other Federal agencies, the DNFSB will request additional evidence that adequate security controls are in place and have been regularly tested, as described in the response to Recommendation 8, below. 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.

Audit 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 December 12, 2014: Agree. Going forward, the DNFSB will request that all external systems operated by Federal agencies for the benefit of the DNFSB must furnish a memo at least annually that confirms that the system is covered by a valid ATO issued by the operating agency, and that as a part of the annual security control testing and contingency plan has been performed. We expect to implement the process for requesting more detailed ATO memos by the end of 2nd 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 ATO's and confirmation that annual contingency plan testing and annual security control testing was performed for the federally operated systems.

Status: Resolved.

Audit 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 December 12, 2014: Agree. The DNFSB agrees to develop a process, plan and schedule for authorizing contractor-operated systems in accordance with FISMA and the NIST FedRAMP. For those contractor-operated systems that are also cloud-based systems, the DNFSB will leverage the FedRAMP process to authorize systems. 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.