Defense Nuclear Facilities Safety Board
Washington, DC 20004-2901

Office of the Inspector General

November 19, 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 NOVEMBER 4, 2015

Attached is the Office of the Inspector General's analysis and status of recommendations as discussed in the Board's response dated November 4, 2015. Based on this response, recommendations 1, 3, 5, 6, and 8 are closed and recommendations 2, 4, 7, and 9 remain resolved. Please provide an updated status of the resolved recommendations by April 29, 2016.

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 November 4, 2015: An annual Security Assessment was completed by external assessor, The Veris Group, on 10/21/2015. The assessment included testing for new and changed NIST controls from SP 800-53, Revision 4, Security control enhancements not tested during the 2012 security assessment, controls impacted by changes to the GSS environment since the security assessment conducted in 2012, and controls associated with the closed Plan of Action and Milestones (POA&M) items. These items will be tested annually as required by NIST 800-53, Revision 4.

The external assessor reviewed all of the controls in our SSP and recommended that an authorization of the DNFSB GSS LAN be granted.

Attached below are the external assessor's Security Assessment Report (SAR) and the updated version of OP 411.2-1, Certification and Accreditation Operating Procedures and the referenced Security Authorization Handbook that requires annual security control testing. We request closure of this recommendation based on the evidence provided.

Recommendation 1 (cont.):

OIG Analysis:	OIG reviewed the external assessor's Security Assessment Report, and the updated version of OP 411.2-1, Certification and Accreditation Operating Procedures and the Security Authorization Handbook that requires annual security testing. OIG determined that the security control assessment tested the minimum controls as outlined in the recommendation. This recommendation is therefore considered closed.
Status:	Closed.

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 November 4, 2015:	The System Characterization Document, the System Security Plan and the Security Authorization Handbook have been updated. The SAR includes the risk assessment and has been finalized by the Veris Group. The updated authorization package is being prepared for final approval. Supporting documentation is attached, and the SAR and Security Authorization Handbook included for recommendation #1. Implementation of this recommendation is still in progress.
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 November 4, 2015:	A security risk assessment was completed by the Veris Group on 10/21/2015 and they created new POA&Ms based on their findings. DNFSB is using the attached procedures to mitigate the POA&M findings from the SAR. (Please see OP-411.2-1 and the Security Authorization Handbook included in recommendation #1.) We request closure of this recommendation based on the evidence provided.
OIG Analysis:	Based on the documents provided, OIG received verification that the risk assigned to the controls impacted by the error were reevaluated and the POA&M was updated as needed. This recommendation is therefore considered closed.
Status:	Closed.

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 November 4, 2015:	The DNFSB is actively mitigating the findings identified in the SAR and related POA&M, and will update the SSP. We anticipate completing the update by 3rd Quarter FY 2016. Implementation of this recommendation is still in progress.
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 November 4, 2015:	Attached are the POA&M management procedures that have been developed, updated, and were approved 8/26/15. DNFSB is currently using these procedures to mitigate the POA&M findings from the SAR. We request closure of this recommendation based on the evidence provided above.
OIG Analysis:	OIG reviewed the attached management procedures and determined that POA&M management procedures were developed, documented, and implemented. This recommendation is therefore considered closed.
Status:	Closed.

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 November 4, 2015:	Attached is the new list of POA&Ms that was created based on the SAR findings.
OIG Analysis:	OIG reviewed the updated POA&M and determined that it included all known vulnerabilities and contained actual completion dates for the completed POA&M activities. This recommendation is therefore considered closed.
Status:	Closed.

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 November 4, 2015:	Language documenting additional oversight of Federal systems was incorporated into the updated OP 411.2-1 that includes the new Security Authorization Handbook as an Appendix, which is attached below. Language documenting authorization of contractor systems and a schedule to authorize existing contractor systems are still being developed and is expected to be completed in 2nd quarter FY 16.
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 November 4, 2015:	The DNFSB issued N-411.2-1.1, dated 7/6/2015, to address the additional ATO information requested. This language was subsequently incorporated into the updated OP 411.2-1 that includes the new Security Authorization Handbook as an Appendix. We request closure of this recommendation based on the evidence provided.
OIG Analysis:	OIG reviewed the supporting evidence and determined that the language requesting confirmation of annual contingency plan testing and annual security control testing for those systems was incorporated. This recommendation is therefore considered closed.
Status:	Closed.

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 November 4, 2015:	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 2nd Quarter FY 2016.
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.