DEFENSE NUCLEAR FACILITIES SAFETY BOARD
WASHINGTON, D.C. 20004-2901

OFFICE OF THE INSPECTOR GENERAL

November 10, 2016

MEMORANDUM TO: Mark T. Welch
General Manager

Katherine Herrera
Deputy General Manager

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: INDEPENDENT EVALUATION OF DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016 **(REDACTED FOR PUBLIC RELEASE)** (DNFSB-17-A-02)

The Office of the Inspector General (OIG) conducted this independent evaluation of the Defense Nuclear Facilities Safety Board's (DNFSB) implementation of the Federal Information Security Modernization Act of 2014 (FISMA 2014) for fiscal year (FY) 2016 to determine the effectiveness of its information security program and practices. In FY 2016, DNFSB completed implementation of all recommendations from the FY 2014 evaluation. As implementation of these recommendations occurred less than 6 months ago, there is not sufficient information to measure their effectiveness. Therefore, there are no new findings or recommendations for FY 2016.

BACKGROUND

On December 18, 2014, the President signed FISMA 2014, reforming the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's OIG or by an independent external auditor.[1]

In 1988 Congress (PL 100-456) created DNFSB as an independent Executive Branch agency to identify the nature and consequences of potential threats to public health and safety at the Department of Energy's defense nuclear facilities, elevate those issues to the highest levels of authority, and inform the public. In operation since October 1989, DNFSB reviews and evaluates the content and implementation of health and safety standards, as well as other requirements, relating to the design, construction, operation, and decommissioning of the Department's defense nuclear facilities.

[1] While FISMA uses the language "independent external auditor," OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, clarified this requirement by stating, "Within the context of FISMA, an audit is not contemplated. By requiring an evaluation but not an audit, FISMA intended to provide Inspectors General some flexibility….."

The U.S. Nuclear Regulatory Commission (NRC) Inspector General holds the position of Inspector General for DNFSB.[2] The NRC OIG retained Richard S. Carson & Associates, Inc. (Carson & Associates), to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2016. This report presents the results of that independent evaluation. Carson & Associates will also submit responses to the Office of Management and Budget's (OMB) annual FISMA reporting questions for OIGs via OMB's automated collection tool in accordance with OMB guidance.

OBJECTIVE

The evaluation objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2016.

FINDING

In FY 2016, DNFSB completed implementation of all nine recommendations from the FY 2014 evaluation (five in November 2015, two in July 2016, and the final two at the end of fieldwork for this year's assessment). As implementation of these recommendations occurred less than 6 months ago, there is not sufficient information to measure their effectiveness. Therefore, there are no new findings or recommendations for FY 2016.

[2] The Consolidated Appropriations Act, 2014 (Public Law 113-76), signed January 17, 2014, provided that the Inspector General of the Nuclear Regulatory Commission (NRC) is authorized to exercise the same authorities with respect to the Board as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App.) with respect to the NRC.

Progress on Implementing FY 2014 Recommendations for Continuous Monitoring

The FY 2014 independent evaluation had two recommendations regarding continuous monitoring:

- Perform an annual security control assessment of the DNFSB general support system (GSS).
- Update the GSS security authorization documentation (e.g., security plan, risk assessment, security assessment report) as required.

DNFSB engaged an external security control assessor to perform a full security assessment of the GSS. The testing was performed in September 2015, and a full authorization to operate (ATO) package was delivered in November 2015. The next annual assessment is scheduled for the end of calendar year 2016. The slight delay is necessary so that DNFSB can complete an Information Technology (IT) project prior to performing the testing.

An updated security assessment report and risk assessment were delivered with the ATO package in November 2015. DNFSB updated the system security plan and system characterization document for the GSS to reflect changes to DNFSB's IT infrastructure and to update all of the controls to those contained in National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Progress on Implementing FY 2014 Recommendations for the NIST Risk Management Framework (RMF)

The FY 2014 independent evaluation had two recommendations regarding the NIST Risk Management Framework (RMF):

- Reevaluate the risk assigned to the controls impacted by an error in the 2012 GSS risk assessment and update the plan of action and milestones (POA&M) as needed.

- Update the GSS system security plan to document accepted risk.

A risk assessment of all controls was conducted as part of the full security assessment of the GSS performed in September 2015. The full ATO package was delivered in November 2015. The system security plan was updated subsequent to the completion of the ATO to document accepted risk.

In addition, the OP-411.2-1 *Information Systems Risk Management Framework and Security Authorization Handbook* was updated in July 2016, and is available on DNFSB's intranet. The Handbook provides guidance on implementing the RMF and the security authorization process within DNFSB.

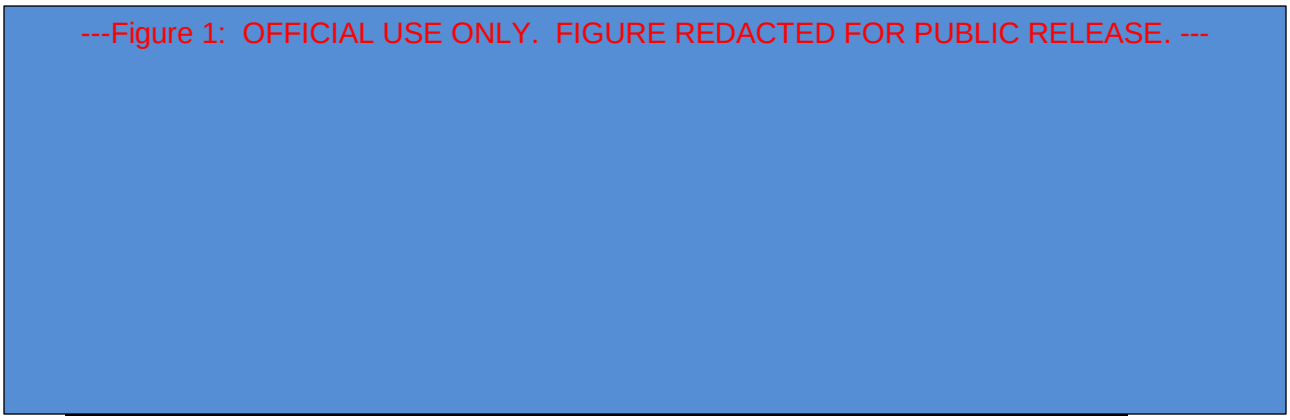
Progress on Implementing FY 2014 Recommendations for POA&M Management

The FY 2014 independent evaluation had two recommendations regarding POA&M management:

- Develop, document, and implement POA&M management procedures.
- Update the POA&M to include all known vulnerabilities and actual completion dates for completed POA&M items.

POA&M management procedures are included in the *Information Systems Risk Management Framework and Security Authorization Handbook*, which is an attachment to OP-411.2-1. A new POA&M was created as a result of the full security assessment of the GSS performed in September 2015.
Progress on remediating POA&M items are reviewed and discussed during monthly Configuration Control Board meetings. Figure 1 summarizes DNFSB's

progress in remediating POA&M items resulting from the full security assessment of the GSS performed in September 2015.



Source: OIG-generated figures from analysis of DNFSB POA&M.

Progress on Implementing FY 2014 Recommendations for Oversight of Contractor Systems

DNFSB has 12 contractor systems, 7 of which are operated by other Federal agencies and 5 by a commercial vendor. Of the five contractor-operated systems, three are considered cloud-based services.

The FY 2014 independent evaluation had three recommendations regarding oversight of contractor systems:

- Develop, document, and implement procedures for performing oversight of systems operated by contractors and other Federal agencies.
- 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.
- Develop a plan and schedule for authorizing contractor-operated systems, including cloud-based systems, in accordance with FISMA, the NIST RMF, and the Federal Risk and Authorization Management Program.

In July 2015, DNFSB issued Notice N-411.2-1.1, which describes the responsibilities and procedures for ensuring IT systems operated by other Federal agencies are properly authorized to operate. The content of N-411.2-1.1 was incorporated into the *Information Systems Risk Management Framework*

and Security Authorization Handbook when it was published as an attachment to OP-411.2-1 in August 2015. Procedures for oversight of federally operated systems were expanded and procedures for oversight of contractor-operated systems were added to the *Information Systems Risk Management Framework and Security Authorization Handbook* in July 2016.

The expanded procedures for oversight of federally operated systems are not yet fully implemented. As a result, DNFSB did not provide the required documentation for these systems for the FY 2016 evaluation.

DNFSB has developed a plan and schedule for authorizing their five contractor-operated systems, including cloud-based systems.

BOARD COMMENTS

A discussion draft of this report was provided to the agency prior to an exit conference held on November 2, 2016. At this meeting, agency management stated their general agreement with the report and opted not to provide formal comments for inclusion in this report.

SCOPE AND METHODOLOGY

Scope

The evaluation focused on reviewing DNFSB's implementation of FISMA 2014 for FY 2016. The evaluation included an assessment of the effectiveness of DNFSB's information security policies, procedures, and practices, and a review of information security policies, procedures, and practices of a representative subset of DNFSB's information systems, including contractor systems and systems provided by other Federal agencies. The FY 2016 evaluation team reviewed the authorization package for the DNFSB GSS, as well as an updated system security plan and system characterization document. As in prior years, there was not sufficient information about DNFSB's use of contractor systems and/or systems provided by other Federal agencies to select any contractor systems for evaluation in FY 2016.

The evaluation was conducted at DNFSB headquarters from July 2016 through October 2016. Any information received from DNFSB subsequent to the completion of fieldwork was incorporated when possible. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, evaluators were aware of the possibility of fraud, waste, and abuse in the program.

Methodology

Carson & Associates conducted an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2016. In addition to an assessment of the effectiveness of DNFSB's information security policies, procedures, and practices, the evaluation included an assessment of the following topics specified in OMB's FY 2016 Inspector General FISMA Reporting Metrics:

- Risk Management, including Plan of Action and Milestones.
- Contractor Systems.
- Configuration Management.
- Identity and Access Management, including Remote Access Management.
- Security and Privacy Training.
- Information Security Continuous Monitoring.
- Incident Response Program.
- Contingency Planning.

To conduct the independent evaluation, the team reviewed the following:

- DNFSB policies, procedures, and guidance specific to DNFSB's information security program and its implementation of FISMA 2014, and to the eight topics specified in OMB's reporting metrics.

All analyses were performed in accordance with guidance from the following:

- NIST standards and guidelines.
- Council of the Inspectors General on Integrity & Efficiency, *Quality Standards for Inspection and Evaluation*, January 2012.
- DNFSB information systems security program policies, processes, procedures, standards, and guidelines.
- NRC OIG guidance.

The evaluation work was conducted by Jane M. Laroussi, CISSP, from Carson & Associates.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TTY/TDD: 7-1-1 or 1-800-201-7165

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.