OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015

DNFSB-16-A-03

November 12, 2015

All publicly available OIG reports (including this report) are accessible through NRC's Web site at
http://www.nrc.gov/reading-rm/doc-collections/insp-gen

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

OFFICE OF THE
INSPECTOR GENERAL

November 12, 2015

MEMORANDUM TO: Mark T. Welch
General Manager

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

SUBJECT: INDEPENDENT EVALUATION OF THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD'S (DNFSB) IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 for FISCAL YEAR 2015 (DNFSB-16-A-03)

Attached is the Office of the Inspector General's (OIG) report titled *Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act of 2014* [FISMA 2014] *for Fiscal Year 2015*. The purpose was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2015.

The report presents the results of the evaluation. As there were no new findings for FY 2015, this report does not contain additional recommendations to improve DNFSB's implementation of FISMA 2014. Following the November 10, 2015, exit conference, DNFSB staff indicated that they had no formal comments for inclusion in this report.

We appreciate the cooperation extended to us by members of your staff during the evaluation. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated

cc: Rosalind Howard

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

DNFSB-16-A-03

November 12, 2015

Results in Brief

Why We Did This Review

The Federal Information Security Modernization Act of 2014 (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 Office of the Inspector General (OIG) or by an independent external auditor. The Office of Management and Budget (OMB) requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

The evaluation objective was to perform an independent evaluation of the Defense Nuclear Facilities Safety Board's (DNFSB) implementation of FISMA 2014 for FY 2015.

Independent Evaluation of DNFSB's Implementation of FISMA 2014 for Fiscal Year 2015

What We Found

In January 2013, DNFSB issued a directive and operating procedure for implementing its information systems security program (ISSP). The FY 2014 independent evaluation found that the majority of the policies and procedures supporting DNFSB's ISSP are draft documents and, therefore, have not been fully implemented. The FY 2014 independent evaluation identified the following ISSP weaknesses, resulting in recommendations:

- Continuous monitoring is not performed as required.
- The security assessment and authorization of DNFSB's general support system did not follow the NIST risk management framework .
- DNFSB's plan of action and milestones management is inadequate.
- Oversight of systems operated by contactors or other agencies is inadequate.

What We Recommend

DNFSB has not completed implementation of any of the recommendations from FY 2014, but has made some progress in addressing the findings. There are no new findings for FY 2015.

Management stated their general agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS i

I. BACKGROUND 1

II. OBJECTIVE 2

III. FINDINGS 2

A. Continuous Monitoring Is Not Performed as Required 3

B. The NIST RMF Was Not Followed 4

C. POA&M Management Is Inadequate 5

D. Oversight of Contractor Systems Is Inadequate 6

IV. CONSOLIDATED LIST OF RECOMMENDATIONS 8

V. DNFSB COMMENTS 9

APPENDIX

OBJECTIVE, SCOPE, AND METHODOLOGY 10

TO REPORT FRAUD, WASTE, OR ABUSE 13

COMMENTS AND SUGGESTIONS 13

ABBREVIATIONS AND ACRONYMS

ATO	Authorization to Operate
DNFSB	Defense Nuclear Facilities Safety Board
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GSS	General Support System
ISSP	Information Systems Security Program
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SP	Special Publication

I. BACKGROUND

On December 18, 2014, the President signed the Federal Information Security Modernization Act of 2014 (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 Office of the Inspector General (OIG) or by an independent external auditor.[1] Office of Management and Budget (OMB) memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2015, requires OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

Congress in 1988 (PL 100-456) created the Defense Nuclear Facilities Safety Board (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., to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for fiscal year (FY) 2015. This report presents the results of that independent evaluation. Carson & Associates will also submit responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool in accordance with OMB guidance.

II. OBJECTIVE

The evaluation objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2015. The report appendix contains a description of the evaluation objective, scope, and methodology.

III. FINDINGS

DNFSB has issued two documents for implementing its information systems security program (ISSP) – Directive D-411.2, *Information Systems Security Program* (approved January 22, 2013), and Operating Procedure OP-411.2-1, *Information Systems Security Program Certification and Accreditation Operating Procedures* (recently updated and approved August 26, 2015). The FY 2014 independent evaluation found that the majority of the policies and procedures supporting DNFSB's ISSP are draft documents and therefore, have not been fully implemented.

The FY 2014 independent evaluation identified the following ISSP weaknesses, resulting in recommendations:

- Continuous monitoring is not performed as required.
- The security assessment and authorization of DNFSB's general support system (GSS) did not follow the National Institutes of

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

Standards and Technology (NIST) risk management framework (RMF).

- DNFSB's plan of action and milestones (POA&M) management is inadequate.

- Oversight of systems operated by contactors or other agencies is inadequate.

DNFSB has not completed implementation of any of the recommendations from FY 2014, but has made some progress in addressing the findings. There are no new findings for FY 2015.

A. Continuous Monitoring Is Not Performed as Required

Step 6 of the NIST RMF, ongoing or continuous monitoring, is a critical part of organization-wide risk management. A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. DNFSB's ISSP, as outlined in D-411.2 and OP-411.2-1, includes requirements for the monitoring of information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. DNFSB's GSS was issued an authorization to operate (ATO) October 3, 2012; however, the FY 2014 independent evaluation found that the required continuous monitoring activities have not been performed, as DNFSB has not fully implemented an enterprise-wide continuous monitoring program. As a result, DNFSB cannot ensure the effectiveness of the GSS information security controls.

Progress on Implementing FY 2014 Recommendations

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

- Perform an annual security control assessment of the GSS.

- Update the GSS security authorization documentation (e.g., security plan, risk assessment, security assessment report) as required.

DNFSB has engaged an external security control assessor to perform a full security assessment of the GSS. The testing began in September 2015, with an expected final delivery of a full ATO package by the end of October 2015. This did not occur at the time of our evaluation.

DNFSB has made an interim update to the system security plan and system characterization document for the GSS to reflect changes to DNFSB's information technology infrastructure and to update all of the controls to those contained in NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

In addition, DNFSB has issued an updated Continuous Monitoring Strategy, which is currently in internal review.

B. The NIST RMF Was Not Followed

The NIST RMF is a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Step 4 is to assess the system's security controls and Step 5 is to authorize the system to operate. OP-411.2-1 describes the procedures for assessing security controls and authorizing systems to operate. DNFSB's GSS was issued an ATO on October 3, 2012; however, during the FY 2014 independent evaluation, a review of the authorization package documents found that key elements of the NIST RMF were not followed. As a result, DNFSB's risk response to the findings from the system authorization may be inadequate.

Progress on Implementing FY 2014 Recommendations

The FY 2014 independent evaluation had two recommendations regarding the NIST RMF:

- Reevaluate the risk assigned to the controls impacted by the error in the 2012 GSS risk assessment and update the 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. The full ATO package was expected to be delivered by the end of October 2015 that would have included an updated system security plan.

In addition, DNFSB recently updated OP-411.2-1 to include a new Information Systems Risk Management Framework and Security Authorization Handbook as an attachment. The updated version, including the new Handbook, was approved August 26, 2015, and is available on DNFSB's intranet.

C. POA&M Management Is Inadequate

FISMA, OMB, and NIST define the requirements for a POA&M process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. The POA&M was updated when DNFSB's GSS was authorized to operate on October 3, 2012. However, the FY 2014 independent evaluation found that the POA&M has not been updated as required, does not include all known security weaknesses, and is missing required information. POA&M management is inadequate because DNFSB has not developed policies and procedures for POA&M management. As a result, the POA&M is not effective at monitoring the progress of corrective efforts relative to known weaknesses in information technology security controls and therefore does not provide an accurate measure of security program effectiveness.

Progress on Implementing FY 2014 Recommendations

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 new Information Systems Risk Management Framework and Security Authorization Handbook, which is an attachment to the recently updated OP-411.2-1. Note that the new Handbook was not received in time for the evaluation team to review to determine if the POA&M management procedures are effective.

Due to errors in the prior risk assessment of the GSS (identified during the FY 2014 independent evaluation), DNFSB has not updated the POA&M and is waiting for the results of the external security control testing. The external assessor has been tasked to review items on the current POA&M to determine whether the issues are still valid or have been resolved.

D. Oversight of Contractor Systems Is Inadequate

FISMA 2014 requires agencies to ensure the adequate protection of agency information, including information collected or maintained by contractors, as well as information systems operated by contractors on the agencies' behalf. DNFSB has 13 contractor systems, 7 of which are operated by other Federal agencies and 6 by a commercial vendor. Of the six contractor-operated systems, four are considered cloud-based services. In FY 2014, DNFSB obtained copies of the ATO memoranda for all but one of the agency-operated systems. However, the FY 2014 independent evaluation found that DNFSB has not authorized any of the contractor-operated systems in accordance with FISMA, NIST RMF, and the Federal Risk and Authorization Management Program (FedRAMP). Oversight of contractor systems is inadequate because DNFSB has not developed policies and procedures for oversight of contractor systems.

As a result, DNFSB cannot determine whether systems that are owned or operated by contractors or other entities are compliant with FISMA requirements, OMB policy, applicable NIST guidelines, and FedRAMP.

Progress on Implementing FY 2014 Recommendations

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 FedRAMP.

Procedures for oversight of contractor systems are included in the new Information Systems Risk Management Framework and Security Authorization Handbook, which is an attachment to the recently updated OP-411.2-1. Note that the new Handbook was not received in time for the evaluation team to review to determine if the procedures for oversight of contractor systems are effective.

In July 2015, DNFSB issued Notice N-411.2-1.1, which describes the responsibilities and procedures for ensuring information technology systems operated by other Federal agencies are properly authorized to operate. The content of N-411.2-1.1 was incorporated into the new Information Systems Risk Management Framework and Security Authorization Handbook when it was published as an attachment to the updated OP-411.2-1.

DNFSB is in the process of determining the most effective way to authorize contractor-operated systems.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

There are no new findings for FY 2015; therefore, the OIG is not issuing any new recommendations.

V. DNFSB COMMENTS

A discussion draft of this report was provided to DNFSB prior to an exit conference held on November 10, 2015. At this meeting, DNFSB management stated their general agreement with the findings in this report and opted not to provide formal comments for inclusion in this report.

Appendix

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2015.

Scope

The evaluation focused on reviewing DNFSB's implementation of FISMA 2014 for FY 2015. 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. DNFSB has only one system; however, that system was reviewed in FY 2014 and is currently undergoing re-authorization. Therefore, there was not an updated system authorization package to review. The FY 2015 evaluation team did review an updated system security plan and system characterization document; however, these documents will have additional updates once the re-authorization is completed. As in FY 2014, 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 2015.

The evaluation was conducted at the DNFSB headquarters from June 2015 through September 2015. 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

Richard S. Carson & Associates, Inc., conducted an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2015. 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 2015 Inspector General FISMA Reporting Metrics:

- Continuous Monitoring Management.
- Configuration Management.
- Identity and Access Management.
- Incident Response and Reporting.
- Risk Management.
- Security Training.
- Plan of Action and Milestones.
- Remote Access Management.
- Contingency Planning.
- Contractor Systems.

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 10 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 ISSP policies, processes, procedures, standards, and guidelines.

- NRC OIG guidance.

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

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TDD 1-800-270-2787

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.