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 2017

DNFSB-18-A-02
October 30, 2017

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

October 30, 2017

MEMORANDUM TO: Glenn Sklar
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 2017 (DNFSB-18-A-02)

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 (FISMA) of 2014 for Fiscal Year 2017*.

The report presents the results of the subject evaluation. Following the October 18, 2017, exit conference, DNFSB management indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum.

We appreciate the cooperation extended to us by members of your staff during the audit. 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

Office of the Inspector General

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

DNFSB-18-A-02
October 30, 2017

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 Fiscal Year 2017.

Independent Evaluation of DNFSB's Implementation of FISMA 2014 for Fiscal Year 2017

What We Found

DNFSB has continued to make improvements in its information security program, and has completed implementing the recommendations from previous FISMA evaluations. However, the independent evaluation identified the following security program weaknesses

- Information security program documentation is not up-to-date
- Information system contingency planning needs improvement.

What We Recommend

To improve DNFSB's implementation of FISMA, we make two recommendations. 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. Information Security Program Documentation is Not Up-to-Date 2
B. Information System Contingency Planning Needs Improvement 5
IV. CONSOLIDATED LIST OF RECOMMENDATIONS 9
V. DNFSB COMMENTS 10

APPENDIXES

A. OBJECTIVE, SCOPE, AND METHODOLOGY 11

TO REPORT FRAUD, WASTE, OR ABUSE 13

COMMENTS AND SUGGESTIONS 13

ABBREVIATIONS AND ACRONYMS

DNFSB	The Defense Nuclear Facilities Safety Board
DOE	The Department of Energy
DRP	Disaster Recovery Plan
GSS	General Support System
FISMA 2014	Federal Information Security Modernization Act of 2014
ISCP	Information System Contingency Plan
NIST	National Institute of Standards and Technology
NRC	The Nuclear Regulatory Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
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.

In 1988 Congress (PL 100-456) created the Defense Nuclear Facilities Safety Board (DNFSB) as an independent Executive Branch agency to provide recommendations and advice to the President and the Secretary of Energy in providing adequate protection of public health and safety at the Department of Energy (DOE) defense nuclear facilities. 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 DOE's defense nuclear facilities.

The U.S. Nuclear Regulatory Commission (NRC) Inspector General holds the position of Inspector General for DNFSB.[1] 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) 2017. This report presents the results of that independent evaluation.

[1] The Consolidated Appropriations Act, 2014 (Public Law 113-76), signed January 17, 2014, provided that the Inspector General of the 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.

II. OBJECTIVE

The objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2017.

III. FINDINGS

Information Security Program Weaknesses

While DNFSB has continued to make improvements in its information security program, and has completed implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified the following information security program weaknesses:

- Information security program documentation is not up-to-date.
- Information system contingency planning needs improvement.

A. Information Security Program Documentation is Not Up-To-Date

DNFSB has Directives and Operating Procedures that specify the frequency of reviewing and updating information security program documentation. However, some information security program documentation is not up-to-date. Up-to-date documentation is important for DNFSB staff to effectively implement the DNFSB information security program.

What Is Required

Internal Requirements for Policies and Procedures

DNFSB Operating Procedure OP-21.1-1, *Directive and Supplementary Document Procedures*, requires Directives to be reviewed every 5 years, and supplementary documents every 3 years. The DNFSB Continuous Monitoring Strategy requires security policies and procedures to be reviewed annually. The Chief Information Officer (CIO), Chief Information Security Officer (CISO), and system owner are responsible for security policies and procedures.

The system security plan for the DNFSB General Support System (GSS) requires policies and procedures applicable to the security control families described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, to be reviewed and updated annually. The system security plan references the following specific documents and their review requirements:

- Control CM-1, Configuration Management Policy and Procedures: the configuration management plan will be reviewed annually.
- Control IR-9, Incident Response Plan: the incident response plan will be reviewed annually.
- Control PM-1, Information Security Program Plan: DNFSB Directive 411.2, *Information System Security Program*, will be reviewed annually.
- Control PM-9, Risk Management Strategy: DNFSB risk management strategy, which is located in DNFSB OP 411.2-1, *Information Systems Security Program Certification and Accreditation Operating Procedures*, Attachment A: *DNFSB Information Systems Risk Management Framework and Security Authorization Handbook*, will be reviewed annually.

The *DNFSB Information Systems Risk Management Framework and Security Authorization Handbook* requires the system characterization document for the DNFSB GSS to be reviewed annually.

What We Found

Security Program Documents Are Not Reviewed and Updated Annually As Required

The following DNFSB security program documents have not been reviewed and updated annually as required:

- DNFSB Directive 411.2, *Information System Security Program*, January 22, 2013.
- DNFSB OP 411.2-1, *Information Systems Security Program Certification and Accreditation Operating Procedures*, August 1, 2016, including Attachment A: *DNFSB Information Systems Risk Management Framework and Security Authorization Handbook*, July 2016.
- DNFSB Administrative Policy AP 411.3, *Information Systems Authentication Policy*, November 29, 2002
- DNFSB GSS Configuration Management Plan, August 2016
- DNFSB Incident Response Plan, February 2016
- DNFSB GSS Security Categorization Document, August 2015

Why This Is Important

DNFSB Staff Need Up-to-Date Documentation To Effectively Implement The DNFSB Information Security Program

Up-to-date documentation is important for DNFSB staff to effectively implement the DNFSB information security program. It is also important

for ensuring that the DNFSB information security program aligns with agency and higher-level Federal Government policies, as well as applicable Federal regulations and laws. Further, up-to-date documentation helps ensure consistent IT security practices in the face of staff turnover or changes in IT security positions.

Recommendation

OIG Recommends that DNFSB

1. Develop a schedule for reviewing and updating all required information security program documentation.

B. Information System Contingency Planning Needs Improvement

NIST requires agencies to develop plans and procedures to ensure continuity of operations for information systems that support agency operations and assets. DNFSB defines its contingency planning requirements in the *DNFSB Information Systems Risk Management Framework and Security Authorization Handbook*. DNFSB has developed both a disaster recovery plan and continuity of operations plan for restoration of operational capability at an alternate site. However, DNFSB has not developed an information system contingency plan (ISCP) for the DNFSB GSS. Lack of an ISCP may prevent timely restoration of services in the event of short-term system disruptions that do not require restoration of operational capability at an alternate site.

What Is Required

Federal Requirements for Contingency Planning

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, defines contingency planning as "interim measures to recover information services after a disruption." Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.

An information system contingency plan (ISCP) is not the same as a disaster recovery plan (DRP) or continuity of operations plan (COOP), but may be prepared in coordination with a DRP and COOP. An ISCP provides established procedures for the assessment and recovery of a system following a system disruption and includes key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system.

The ISCP differs from a DRP primarily in that the ISCP procedures are developed for recovery of the system regardless of site or location. A DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. An ISCP can be activated at the system's current location or at an alternate site.

NIST SP 800-53, Revision 4, provides additional guidance on developing an ISCP to include procedures for both information system restoration as well as implementation of alternative mission/business processes when systems are compromised. Procedures can include orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack.

Internal Requirements for Contingency Planning

The *DNFSB Information Systems Risk Management Framework and Security Authorization Handbook* requires an ISCP for all moderate and

high impact systems that includes actions to be implemented when a disruption occurs, the procedures to be taken to mitigate the risks and ensure the availability of the system, and the reconstitution of the system after the disruption.

What We Found

DNFSB GSS Does Not Have an Information System Contingency Plan

The DNFSB GSS does not have an ISCP, contrary to NIST guidance and an internal DNFSB requirement. DNFSB developed the following documents related to contingency planning. Both of these documents discuss restoration of operational capability at an alternate site.

- DNFSB DRP: An information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. This DRP may be supported by multiple ISCPs to address recovery of impacted individual systems once the alternative facility has been established. The DNFSB DRP is based on the DNFSB COOP. The DNFSB DRP is not an ISCP to recover or restore individual systems at the COOP or other alternative facility.

- DNFSB COOP: provides for attaining operational capability within 12 hours and sustaining operations for 30 days or longer in the event of a catastrophic event or a national security emergency affecting the National Capital Region, or any event which precludes the use of the DNFSB headquarters facility.

During the FY 2016 FISMA evaluation, DNFSB stated that an ISCP for the DNFSB GSS was still in draft. The DNFSB system security plan also states that an ISCP is being developed for the system. However, DNFSB has not developed an ISCP for the DNFSB GSS that includes key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system.

Why This Is Important

Timely Restoration of Services May be Impacted

An ISCP provides steps for recovery of a system regardless of site or location, and can be activated at the system's current location or at an alternate site. While DNFSB has documents that describe restoration of operational capability at an alternate site, it does not have an ISCP that describes restoring system components using alternate equipment or performing some or all of the affected business processes using alternate processing (manual) means when restoration at an alternate site is not needed. For example, DNFSB has not documented procedures for contingency events that do not require activation of the DRP and/or COOP, such as the failure of a disk drive or power supply, corruption of a database, or a possible system compromise. Lack of an ISCP may prevent timely restoration of services in the event of short-term system disruptions that do not require restoration of operational capability at an alternate site.

Recommendation

OIG Recommends that DNFSB

2. Develop an information system contingency plan for the DNFSB GSS.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that DNFSB

1. Develop a schedule for reviewing and updating all required information security program documentation.
2. Develop an information system contingency plan for the DNFSB GSS.

V. DNFSB COMMENTS

An exit conference was held with the agency on October 18, 2017. Prior to this meeting, after reviewing a discussion draft, agency management provided comments that have been incorporated into this report, as appropriate. As a result, agency management stated their general agreement with the findings and recommendations and opted not to provide formal comments for inclusion in this report.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2017.

Scope

The evaluation focused on reviewing DNFSB's implementation of FISMA 2014 for FY 2017. The evaluation included an assessment of the effectiveness of the 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 2017 evaluation team reviewed the current DNFSB GSS system security plan, the security assessment report for the FY 2017 annual assessment, and the resulting plan of action and milestones.

The evaluation was conducted at DNFSB headquarters from June 2017 through September 2017. 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 considered 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 2017. In addition to an assessment of the effectiveness of the DNFSB's information security policies, procedures, and practices, the evaluation included an assessment of the following topics specified in OMB's FY 2017 Inspector General FISMA Reporting Metrics:

- Risk Management.
- Configuration Management.
- Identity and Access Management.
- Security Training.
- Information Security Continuous Monitoring.
- Incident Response.
- 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 seven 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 Security Planning and Oversight Branch policies, processes, procedures, standards, and guidelines.
- NRC OIG guidance.

The evaluation work was conducted by Brett Baker, Assistant Inspector General for Audits; Beth Serepca, Team Leader; Kristen Lipuma, Audit Manager; and 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

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.