OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Audit of the Defense Nuclear Facilities Safety Board's Information Security Program

DNFSB-16-A-02

October 28, 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

October 28, 2015

MEMORANDUM TO: Mark T. Welch
General Manager

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

SUBJECT: AUDIT OF THE DEFENSE NUCLEAR FACILITIES SAFETY BOARD'S INFORMATION SECURITY PROGRAM (DNFSB-16-A-02)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of the Defense Nuclear Facilities Safety Board's* [DNFSB] *Information Security Program*.

The report presents the results of the subject audit. Following the October 22, 2015, exit conference, DNFSB staff 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

cc: R. Howard, OGM

Office of the Inspector General

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

OIG-16-A-02
October 28, 2015

Results in Brief

Why We Did This Review

The Defense Nuclear Facilities Safety Board (DNFSB) is an independent organization within the Executive Branch that advises the President and the Secretary of Energy on public health and safety issues at Department of Energy (DOE) defense nuclear facilities. 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 DOE defense nuclear facilities.

DNFSB uses classified and sensitive unclassified information to conduct agency business in support of its mission. Safeguarding both classified and sensitive unclassified information is necessary for protecting national security interests, as well as the safety, security, and privacy of DNFSB employees.

The audit objective was to determine if DNFSB handles classified and sensitive unclassified information in accordance with Federal regulations.

Audit of the Defense Nuclear Facilities Safety Board's Information Security Program

What We Found

DNFSB has appropriate security controls for classified information and some types of sensitive unclassified information such as Personally Identifiable Information. However, opportunities exist to improve DNFSB's internal information security guidance, and to improve access controls over Unclassified Controlled Nuclear Information (UCNI) that is stored on DNFSB's internal SharePoint site.

Federal guidance recommends that documentation of internal controls should be clear and readily available. However, DNFSB's main information security guidance is incomplete and does not address key points for protecting sensitive unclassified information. This occurs because DNFSB has not updated its primary information security guidance since May 2000. DNFSB staff need current and complete guidance to help them carry out their information security responsibilities.

Additionally, Federal regulations require a "need to know" as a condition for routine access to UCNI. However, general computer network access rights allow users to access and manipulate some UCNI documents saved on the agency's internal SharePoint site without establishing a need to know. This occurs because technical controls are not required to manage access to UCNI documents stored on SharePoint. As a result, security-related information is at greater risk of unauthorized disclosure or compromise.

What We Recommend

This report makes recommendations to improve DNFSB's information security guidance and UCNI access controls on its internal SharePoint site. DNFSB management stated their general agreement with the report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

CFR	Code of Federal Regulations
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
PII	Personally Identifiable Information
UCNI	Unclassified Controlled Nuclear Information

I. BACKGROUND

The Defense Nuclear Facilities Safety Board (DNFSB) is an independent organization within the Executive Branch that advises the President and the Secretary of Energy on public health and safety issues at Department of Energy (DOE) defense nuclear facilities. 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 DOE defense nuclear facilities.

DNFSB uses classified and sensitive unclassified information to conduct agency business in support of its mission. Safeguarding both classified and sensitive unclassified information is necessary for protecting national security interests, as well as the safety, security, and privacy of DNFSB employees.

DNFSB Information Security Program

DNFSB's information security program is designed to protect classified and sensitive unclassified information, and generally reflects DOE information security policies and procedures. In addition, DNFSB's policies and procedures focus on protection of classified and sensitive unclassified information at agency headquarters. DNFSB's site representatives at DOE defense nuclear facilities follow DOE and site-specific procedures at their respective locations.

Classified Information at DNFSB

Classified information used by DNFSB staff includes Restricted Data, which pertains to development and use of nuclear weapons.[1] DNFSB staff use classified information for their work, but do not have the authorities required to classify information. Rather, they submit documents to authorized DOE classifiers for information security reviews, and classification if needed.

Sensitive Unclassified Information at DNFSB

DNFSB staff use several types of sensitive unclassified information. Two types of sensitive unclassified information are Personally Identifiable Information (PII) and Unclassified Controlled Nuclear Information (UCNI). PII is information about an individual that is maintained by an agency and may include, but is not limited to, education, financial transactions, medical history, and criminal or employment history. Additionally, PII includes information that can be used to distinguish or trace an individual's identity, such as one's name, social security number, date and place of birth, mother's maiden name, or biometric records. Protecting specific kinds of PII is generally required by various laws, such as the Privacy Act of 1974.

UCNI pertains to the design of facilities that produce or use special nuclear material, unclassified security measures for protecting such facilities and nuclear material contained within those facilities, and unclassified security measures for protecting nuclear material in transit. Unauthorized dissemination of UCNI is prohibited under Section 148 of the Atomic Energy Act, and 10 CFR 1017 prescribes requirements for safeguarding UCNI.

[1] Title 10, Code of Federal Regulations, Part 1016 (10 CFR 1016) addresses safeguards for Restricted Data and Formerly Restricted Data. 10 CFR 1045 addresses classification authorities and training requirements for personnel who may have access to this type of information.

II. OBJECTIVE

The audit objective was to determine if DNFSB handles classified and sensitive unclassified information in accordance with Federal regulations. The report appendix contains information on the audit scope and methodology.

III. FINDINGS

OIG examined DNFSB's policies and procedures for managing classified and sensitive unclassified information. Based on this work, auditors found that DNFSB has appropriate security controls for classified information and some types of sensitive unclassified information such as PII. However, opportunities exist to improve DNFSB's internal information security guidance, and to improve access controls over one type of sensitive unclassified information (specifically, UCNI) that is stored on DNFSB's internal SharePoint site.

A. DNFSB Information Security Guidance Is Incomplete

Federal guidance recommends that documentation of internal controls should be clear and readily available. However, DNFSB's main information security guidance is incomplete and does not address key points for protecting sensitive unclassified information. This occurs because DNFSB has not updated its primary information security guidance since it was issued in May 2000. DNFSB staff need current and complete guidance to help them carry out their information security responsibilities.

What Is Required

Federal Internal Control Guidance

The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*[2] requires that agencies clearly document internal processes with sufficient detail to allow management to effectively monitor agency activities. This documentation must be properly managed, maintained, and made available to meet its intended purpose. In addition, the Office of Management and Budget's *Final Bulletin for Agency Good Guidance Practices* recognizes the value of clearly documenting agency guidance. The Office of Management and Budget maintains that well-designed guidance documents, if used properly, can appropriately direct agency employees and increase efficiency.

What We Found

DNFSB Information Security Policy Is Incomplete

DNFSB's primary information security guidance—Administrative Directive 301-1—establishes policies and procedures for protecting classified information. However, this guidance is incomplete and does not address key points for sensitive unclassified information protection such as management of information security breaches[3] and protecting data that is processed electronically.

[2] GAO-14-704G, September 2014.

[3] DNFSB does have a more current operating procedure—last reviewed in 2012—that specifically addresses protection of the agency's Privacy Act systems of records, which contain PII.

Why This Occurred

DNFSB Information Security Guidance Has Not Been Recently Updated

DNFSB's primary information security guidance (Administrative Directive 301-1) is incomplete because it has not been updated since it was last issued in May 2000.[4] During this audit, DNFSB staff were in the process of drafting a new directive and an operating procedure, which are both intended to supersede Administrative Directive 301-1.

Why This Is Important

DNFSB Staff Need Current and Complete Guidance To Uphold Information Security Responsibilities

Having current and complete guidance is important for DNFSB staff to understand and uphold their information security responsibilities. It is also important for ensuring that routine security practices align with agency and higher-level Federal Government policies, as well as applicable Federal regulations and laws. Further, current and complete guidance helps ensure consistent information security practices in the face of staff turnover or changes in security and information management positions.

Recommendations

OIG recommends that DNFSB

1. Update information security guidance for classified and sensitive unclassified information so that it addresses management of information security breaches and protection of electronically processed information.

[4] DNFSB issued an office procedure in 2014 that mentions employees' general responsibilities to protect classified and sensitive unclassified information. However, this document instructs employees to refer to administrative directives and operating procedures for more specific guidance.

B. Inconsistent Access Controls on DNFSB SharePoint

Federal regulations require a "need to know," among other criteria, as a condition for routine access to UCNI. However, general computer network access rights allow users to access and manipulate some UCNI documents saved on the agency's internal SharePoint site without establishing a need to know specific UCNI in these documents. This occurs because technical controls are not required to manage access to UCNI documents stored on SharePoint. As a result, security-related information is at greater risk of unauthorized disclosure or compromise.

What Is Required

Federal Regulations Require "Need to Know" for Accessing UCNI

The CFR specifies requirements for protecting and controlling access to UCNI. Specifically, it stipulates that personnel must need to know specific UCNI to perform official duties or other Government-authorized activities as a precondition for routine access. Personnel must also meet U.S. citizenship and Government employment criteria, with limited exceptions.[5] Additionally, documents containing UCNI must be stored in a manner that precludes unauthorized disclosure.[6]

What We Found

Inconsistent Use of Technical Access Controls on DNFSB's SharePoint Site

OIG auditors systematically reviewed documents stored on the agency's internal SharePoint site and found inconsistent use of technical access controls to protect documents containing UCNI. Among approximately

[5] 10 CFR 1017.20.

[6] 10 CFR 1017.24.

280 documents that appeared to contain UCNI, auditors found 1 document that was password-protected and, thus, could not be viewed and modified by auditors. However, auditors also found documents containing UCNI that lacked password protection, thereby enabling auditors—or anyone else with similar general network access privileges—to read, edit, download, and transmit such documents. For more information regarding auditors' SharePoint query, refer to the Scope and Methodology section of this report.

Why This Occurred

DNFSB Does Not Require Technical Controls for UCNI Documents Stored on SharePoint

The inconsistent use of technical controls for UCNI documents stored on DNFSB's SharePoint site occurred because these controls are not required by agency policy. Moreover, organizational culture reportedly supports the assumption that agency staff trust one another to enforce the need-to-know principle. DNFSB management also cited challenges in enforcing the need-to-know principle without compromising their technical staff's workflow, which can change their individual requirements for access to specific documents containing UCNI.

Why This Is Important

Security-Related Information Is at Greater Risk of Unauthorized Disclosure or Compromise

UCNI saved on SharePoint without technical access controls based on a user's need to know puts security-related information at greater risk of unauthorized disclosure or compromise. Additionally, a lack of technical controls designed to prevent modification of documents containing UCNI could in turn compromise the integrity and reliability of this information. Moreover, recent Department of Homeland Security best practice guidance recommends that Federal agencies segment their computer networks to mitigate the effects of a breach. Segmentation helps protect

overall network integrity if an isolated portion of the network is compromised.

Recommendations

OIG recommends that DNFSB

2. Implement technical controls in the DNFSB SharePoint site that limit access to UCNI documents on a need-to-know basis.

3. Incorporate into DNFSB policy the requirement for technical controls in SharePoint to control access to UCNI documents on a need-to-know basis.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that DNFSB

1. Update information security guidance for classified and sensitive unclassified information so that it addresses management of information security breaches and protection of electronically processed information.

2. Implement technical controls in the DNFSB SharePoint site that limit access to UCNI documents on a need-to-know basis.

3. Incorporate into DNFSB policy the requirement for technical controls in SharePoint to control access to UCNI documents on a need-to-know basis.

V. DNFSB COMMENTS

A discussion draft of this report was provided to DNFSB prior to an exit conference held on October 22, 2015. DNFSB management provided comments that have been incorporated into this report, as appropriate. As a result, DNFSB management stated their general agreement with the report and will not provide formal comments.

Appendix

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine if DNFSB handles classified and sensitive unclassified information in accordance with Federal regulations.

Scope

The audit reviewed DNFSB's activities related to sensitive unclassified and classified information with special emphasis on procedures and compliance with Federal regulations and policies. OIG conducted this performance audit from June 2015 to September 2015 at DNFSB headquarters in Washington, DC, and at NRC headquarters in Rockville, MD. Internal controls related to the audit objective were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility or existence of fraud, waste, and abuse in the program.

Methodology

To address the audit objective, OIG reviewed Federal regulations and agency guidance including the following:

- CFR sections pertaining to protection of classified information and Unclassified Controlled Nuclear Information, including 10 CFR 1016, 10 CFR 1045, 32 CFR 2001, and 10 CFR 1017.
- National Institute of Standards and Technology, "Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010.
- Government Accountability Office, *Standards for Internal Control in the Federal Government*.
- Department of Homeland Security, "Informational Bulletin: Best Practices to Protect You, Your Network, and Your Information," July 31, 2015.

OIG auditors interviewed DNFSB personnel to obtain their perspectives on how DNFSB manages sensitive unclassified and classified information. Auditors also reviewed DNFSB internal information security guidance, including Administrative Directive 301-1 and Operating Procedure 231.2-1 (Privacy Act and PII protection). Additionally, auditors reviewed DNFSB information security guidance currently in draft version.

OIG auditors observed and analyzed protective measures for storing and processing classified information at DNFSB headquarters, and reviewed training materials that address security of classified and sensitive unclassified information at DNFSB and DOE sites.

OIG auditors obtained general computer network access, and tested access controls over DNFSB's shared drives and internal SharePoint site. Using a search, identify and examine methodology, auditors ran queries designed to find documents containing specific types of sensitive unclassified information, such as PII and UCNI. In cases where queries yielded positive results for UCNI on SharePoint, auditors tested their ability to download documents. For successful downloads, auditors reviewed the documents' security settings.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; Ziad Buhaissi, Senior Auditor; Jenny Cheung, Auditor; and Ebaide Esoimeme, Auditor.

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.