OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Cybersecurity Act of 2015 Audit for DNFSB

DNFSB-16-A-07

August 8, 2016

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

August 8, 2016

MEMORANDUM TO: Mark T. Welch
General Manager

Katherine Herrera
Deputy General Manager

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

SUBJECT: CYBERSECURITY ACT OF 2015 AUDIT FOR DNFSB (DNFSB-16-A-07)

Attached is the Office of the Inspector General's (OIG) audit report titled *Cybersecurity Act of 2015 Audit for DNFSB*.

The report presents the results of the subject audit. Following the August 4, 2016, 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

Office of the Inspector General

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

OIG-16-A-07

August 8, 2016

Results in Brief

Why We Did This Review

The Cybersecurity Act of 2015 was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States. Division N, Section 406, of the Act requires that Inspectors General report on the policies, procedures, and controls to access "covered systems."

Covered systems are defined as a national security system, or a Federal computer system that provides access to personally identifiable information (PII).

The Defense Nuclear Facilities Safety Board (DNFSB) relies on the servicing organizations to properly protect the records, but must review the privacy impact assessment to determine they are using proper controls. However, DNFSB does not review the privacy impact assessment for external organizations.

The audit objective was to evaluate DNFSB's information technology (IT) security policies, procedures, practices, and capabilities as defined in the Cybersecurity Act of 2015 for national security systems and systems that provide access to personally identifiable information (PII) operated by or on behalf of DNFSB.

Cybersecurity Act of 2015 Audit for DNFSB

What We Found

DNFSB's cybersecurity program has established policies, procedures, and controls to access to its "covered systems." However, DNFSB does not comply with all requirements of the Privacy Act of 1974 and the E-Government Act of 2002. Specifically, DNFSB does not

- Conduct required reviews of its systems of record.
- Review privacy impact assessments for external servicing organizations.

This is happening because of a lack of adequate internal policies to implement both laws. As a result, PII may be vulnerable or at risk of unauthorized disclosure.

In addition, OIG reviewed the policies, procedures, and controls in place for DNFSB's local area network that provides access to PII. OIG reviewed the privacy impact assessment for DNFSB's General Support System Local Area Network that maintains PII and the system security plan. Section IV of this report discusses the policies, procedures, and controls.

What We Recommend

This report makes two recommendations to bring DNFSB into compliance with the Privacy Act of 1974 and E-Government Act of 2002. Management stated their general agreement with the finding and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

DNFSB	Defense Nuclear Facilities Safety Board
GSS	General Support System
LAN	Local Area Network
NIST	National Institute for Standards and Technology
OMB	Office of Management and Budget
OIG	Office of the Inspector General
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification

I. BACKGROUND

The Cybersecurity Act of 2015

The Cybersecurity Act of 2015 (Act) was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States. The Act aims to promote and to facilitate sharing of information across entities, both Federal and non-Federal, whose cybersecurity efforts could potentially benefit from greater access to cybersecurity-related information.

Division N, Cybersecurity Act of 2015

The Act at Division N, Section 406 requires that Inspectors General report to the appropriate committees of jurisdiction in the Senate and House of Representatives on the policies, procedures, and controls to access "covered systems." The specific Inspector General reporting requirements of Division N can be found here and is set forth in section IV of this report. Covered systems are defined by the Act as a national security system, or a Federal computer system that provides access to personally identifiable information (PII).

The National Institute for Standards and Technology (NIST) defines PII as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

In addition, the Office of Management and Budget (OMB) guidance defines "information in indentifiable form" as information in an IT (information technology) system or online collection: (i) that directly identified any individual (e.g. name,

address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjuction with other data elements, i.e, indirect identification. (These data elements may include a combination of gender, race, birth, date, geographic indicator, or other descriptors.)

The Privacy Act of 1974.

The Privacy Act of 1974 establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in a system of records by a Federal agency. A system of records is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of record by publication in the Federal Register. This is called a “System of Record Notice.” The Privacy Act provides individuals with a means to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.

E-Government Act of 2002.

The E-Government Act of 2002 requires all Federal agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates PII. A PIA is an analysis of how information is handled to ensure it conforms to requirements for privacy. The assessment determines the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system. Agencies must describe how the government handles information that individuals provide electronically, so that the American public has assurance that personal information is protected.

II. OBJECTIVE

The audit objective was to evaluate the information technology security policies, procedures, practices, and capabilities as defined in the Cybersecurity Act of 2015 for national security systems and systems that provide access to PII operated by or on behalf of the Defense Nuclear Facilities Safety Board (DNFSB).

III. FINDING

DNFSB Does Not Comply with All Requirements of the Privacy Act and E-Government Act

DNFSB does not comply with all requirements of the Privacy Act of 1974 and the E-Government Act of 2002. This is happening because of a lack of adequate internal policies to implement both laws. As a result, PII may be vulnerable or at risk of unauthorized disclosure.

The Cybsecurity Act required Inspectors General to look at Federal computer systems that provide access to PII. In reviewing DNFSB's systems that contain PII, the Inspector General reviewed the E-Government Act and Privacy Act and determined DNFSB is not in full compliance with these acts.

What Is Required

OMB Criteria

OMB published guidance that Federal agencies must follow when implementing the Privacy Act of 1974 and the E-Government Act of 2002.

OMB A-130, Appendix I

OMB A-130, Appendix I, describes Federal agency responsibilities for implementing the reporting and publication requirements of the Privacy Act. Appendix I requires agencies to biennially review each system of records notice to ensure that it accurately describes the system of records. If a new or altered system is identified, this must be reported. Where minor changes are needed, (e.g. a system manager changes), agencies must ensure that an amended notice is published in the Federal Register.

The E-Government Act of 2002

The E-Government Act requires all Federal agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII, or for a new aggregation of information that is collected, maintained, or disseminated using information technology. The PIA for DNFSB's GSS LAN[1] states "...[T]he Board [DNFSB] relies on external servicing organizations to properly protect records but reviews appropriate security authorizations and PIAs (Privacy Impact Assessments) to determine they are using proper controls."

[1] GSS LAN stands for General Support Service Local Area Network. The GSS LAN is an Ethernet-based network that connects all user workstations with centralized file servers used to store data and host applications.

OMB Guidance M-03-22

OMB Guidance M-03-22 to agencies addresses implementing the privacy provisions of the E-Government Act. It requires agencies to conduct PIAs for electronic information systems and collections and, in general, make them publicly available.

What We Found

DNFSB does not comply with all requirements of the Privacy Act and the E-Government Act.

DNFSB does not conduct biennial reviews of its systems of records.

DNFSB does not conduct biennial reviews of its systems of records. DNFSB's last system of records notice was reported in the Federal Register in 2011. While their systems of records are currently undergoing review, no review of the systems was conducted between July 2011 through March 2016.

DNFSB does not review PIAs for external servicing organizations

DNFSB does not review PIAs for external servicing organizations to ensure they are using proper privacy controls. For externally hosted systems that contain PII of employees and its contractors, DNFSB relies on the servicing organizations to properly protect the records. However, DNFSB is required to review the appropriate security authorizations and PIAs to determine that these external servicing organizations are using

proper controls. While DNFSB is reviewing the security authorizations, they are not reviewing the PIAs to ensure proper privacy controls are used. External systems[2] relied upon by DNFSB include the Government Benefits Retirement Calculator, Financial Tracking System, iLMS (inspired eLearning), Bureau of Fiscal Services, and USDA's Concur Travel System.

The PIA for the GSS LAN is Not Publicly Available

Furthermore, at the end of fieldwork on this audit, the PIA for the GSS LAN was not publicly available. It was available to all DNFSB staff internally, but was not posted on the public Web site. DNFSB has since posted it on the public Web site.

Why This Occurred

DNFSB lacks adequate and up-to-date policies and procedures for implementing the Privacy Act and the E-Government Act.

DNFSB has Operating Procedure 231.2-1, "Privacy Act Operating Procedures," that was approved on August 31, 2009, and was scheduled to be reviewed in August 2012. This procedure does not comply with all requirements of OMB Circular A-130, Appendix I and the E-Government Act as follows:

- It does not include the requirement to conduct a biennial review of all systems of records.
- OP 231.1-2 states "Completed PIAs [Privacy Impact Assessments] will be made available to the public, if required, by being posted to

[2] External systems contain PII and are operated by other Federal agencies or contractor.

the Board's [DNFSB's] Web site." But, it fails to assign responsibility.

- OP 231.1-2 was published in August 2009 and was set to be reviewed in August 2012; however, it has yet to be reviewed.

In addition, the GSS LAN PIA lacks specificity in assigning responsibility for reviewing the privacy controls for external systems. The document merely says it will be done, without assigning responsibility.

Lastly, DNFSB has a Draft Handbook for Safeguarding Sensitive Personally Identifiable Information, dated October 2015. However, it has not been adopted as formal guidance or distributed to staff.

Why This Is Important

Without adequate policies and procedures for implementing the Privacy Act and the E-Government Act, PII may be vulnerable or at risk of unauthorized disclosure.

Without a biennial review of its system of records, DNFSB is overlooking changes to their systems that are required to be reported. Thus, individuals whose information is collected, do not have current information on what each system contains. These individuals have the right to know how their personal information is collected, stored, and shared.

In addition, information on external systems may be vulnerable to unauthorized disclosure. Per the GSS LAN PIA, DNFSB is required to review the PIA for external systems to ensure the proper privacy controls are being

used. Without this additional layer of review, DNFSB may not be aware if these servicing agencies have adequate privacy controls for information stored on their systems. Thus, the information may be vulnerable to unauthorized disclosure.[3]

Lastly, because DNFSB did not make the PIA publicly available, there was a lack of transparency. Transparency gives the American public assurance that personal information is appropriately protected.

Recommendations

OIG Recommends that the DNFSB

1. Revise current policies and procedures to comply with the Privacy Act of 1974 Requirements and E-Government Act of 2002, and assign responsibility for complying with those requirements.

2. Finalize, publish, and disseminate the Draft Handbook for Safeguarding Personally Identifiable Information, dated October 2015.

[3] The new Information Systems Risk Management Framework and Security Authorization Handbook, dated July 2016, requires that system owners request the privacy impact assessment and privacy incident response plans for external systems. It also requires the Change Control Board to review those documents and document the results of the review in determining whether to authorize use of the system.

IV. Policies, Procedures, and Controls per the Cybersecurity Act of 2015

A. Statutory Basis for Reporting.

Division N of the Cybersecurity Act of 2015, Section 406, requires Inspectors General to report on covered systems[4]. OIG is required to report on:

1. A description of the logical access control policies and practices used by DNFSB to access covered systems, including whether appropriate standards were followed.
2. A description and list of the logical access controls and multi-factor authentication used by DNFSB to govern access to covered systems by privileged users.
3. A description of information security management practices used by DNFSB.
4. A description of the policies and procedures of DNFSB with respect to ensuring that entities, including contractors, that provide services to DNFSB are implementing information security management practices used by DNFSB.

B. Logical access, policies and practices used to access covered systems, and appropriate standards.

DNFSB's Directive 411.2 Information Systems Security Program. DNFSB's Information Systems Security Program establishes policy,

[4] Division N of the Cybersecurity Act of 2015, Section 406 can be accessed at https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf

requirements, and responsibilities for ensuring an adequate level of information security for all unclassified information collected, created, processed, transmitted, stored, or disseminated on DNFSB's internal and external information systems. DNFSB implements security requirements to protect the confidentiality, integrity, and availability of Federal information systems and the information processed, stored, and transmitted by these systems. Further, DNFSB complies with the security controls articulated in the National Institute for Standards and Technology (NIST) 800-53 Revision 4.

C. List of the logical access controls and multi-factor authentication that govern access to covered systems.

DNFSB's Administrative procedure 411.3 Information Systems Authentication Policy. DNFSB's Information Systems Authentication Policy establishes minimum requirements for the identification and authentication of users when accessing unclassified DNFSB information systems.

All DNFSB members and contractors must use their Personal Identity Verification (PIV) card and a pin number to gain access to the GSS LAN and SharePoint. DNFSB also implements role based access control for all systems and users are assigned to a single "users" group. Privileged access is restricted to separate administrator accounts. All local and remote system access to the GSS LAN requires users to uniquely identify and authenticate themselves via Active Directory.[5]

[5] Active Directory is a database that keeps track of all organizational user accounts and passwords.

D. Information security management practices used by DNFSB.

Directive 412.1, Acceptable Personal Use of Information Technology Services. Employees and contractors are required to use DNFSB's Information Technology Services in an effective, efficient, ethical, and lawful manner. Employees and contractors are authorized to use DNFSB's Information Technology Services for limited personal use as long as it does not interfere with DNFSB's mission or operation and does not violate the standards of ethical conduct for employees of the executive branch.

DNFSB requires that Privacy Act systems of records and files containing PII be strictly limited to the number of staff and contractors with access to PII and to those with an authorized "need-to-know" in order to perform their official duties. DNFSB prevents access to Privacy Act system of records and PII data stored in electronic format from outside DNFSB's protected network. Additionally, DNFSB restricts the operation of selected electronic Privacy Act system of records and PII data to a secure, stand-alone work station with enhanced protection features.

DNFSB implements NIST security technical controls for moderate impact information systems to include enhanced password protection, access monitoring systems, encrypting password files, encrypting PII data, user warning messages, and notifications of inclusion of PII data before allowing access. A written approval is required from the Chairman or General Manager before encrypted or similarly protected PII in electronic formats or un-redacted PII in paper form can be removed from DNFSB offices.

Operating Procedure 213.2-1 requires that an unauthorized disclosure of any information from a systems of record by any means of communication to a person, or to another agency, should be reported immediately to the DNFSB's General Manager to determine further action. DNFSB is required to report all incidents involving PII breaches, in any format, to the US-CERT within one hour of discovery/detection.

E. A description of DNFSB policies and procedures to ensure that entities, including contractors, that provide services to DNFSB are implementing information security management practices used by DNFSB.

Operating Procedure 411.2-1, Information Systems Security Program Certification and Accreditation Operating Procedures. This operating procedure facilitates the implementation of the Risk Management Framework and security authorization processes within DNFSB.

Operating Procedure 231.2-1, Privacy Act Operating Procedures. This operating procedure requires all DNFSB employees and contractors to share in the responsibility to protect the information in DNFSB's Privacy Act systems of record and PII from unauthorized disclosure or compromise.

DNFSB relies on external servicing organizations to properly protect records on external systems and reviews appropriate security authorizations and privacy impact assessments to determine if they are using proper controls. However, as indicated in Section III of this report, DNFSB is not conducting required reviews of the privacy impact assessments of the external systems it uses.

V. DNFSB COMMENTS

A discussion draft of this report was provided to DNFSB prior to an exit conference held on August 4, 2016. 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 A

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to evaluate the information technology security policies, procedures, practices, and capabilities as defined in the Cybersecurity Act of 2015 for national security systems and systems that provide access to PII operated by or on behalf of DNFSB.

Scope

The audit focused on the policies, procedures, and controls used to access DNFSB systems that provide access to PII. This audit does not address the policies, procedures, and controls used to access any national security systems.

We conducted this performance audit at DNFSB headquarters in Washington, D.C. from March 2016 to June 2016. OIG also reviewed and analyzed internal controls related to the audit objective. Throughout the audit, auditors were aware of the possibility of fraud, waste, and abuse in the program.

Methodology

OIG reviewed Federal laws and guidance, including:

- The Privacy Act of 1974, 5 U.S.C sec 552a.
- The E-Government Act of 2002.
- OMB A-130 Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.
- OMB Guidance M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

- National Institute for Standards and Technology (NIST) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

To understand the policies and procedures in place for logical access controls on systems that provide access to PII, OIG reviewed internal documents including:

- Directive 411.2, "Information Systems Security Program."
- Administrative Policy 411.3, "Information Systems Authentication Policy."
- Operating Procedure 411.2-1, "Information Systems Security Program Certification and Accreditation Operating Procedures."
- Operating Procedure 231.2-1, "Privacy Act Operating Procedures."

OIG interviewed DNFSB staff and management to gather information on logical access controls for systems that have access to PII. Auditors interviewed personnel from the Office of General Manager and the Office of General Counsel. Additionally, OIG tested access controls on the "H: Drive" in order to ensure that proper controls were in place and restricted access to only those with the proper authorization who need access to the information as part of their official duties.

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; Kristen Lipuma, Audit Manager; Ziad Buhaissi, Senior Auditor; Ebaide Esoimeme, Auditor; Janelle Wiggs, Auditor; and Chanel Stridiron, 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.