OFFICE OF THE INSPECTOR GENERAL

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

Evaluation of NRC's Shared "S" Drive

OIG-18-A-06
December 21, 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

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

December 21, 2017

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

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

SUBJECT: EVALUATION OF NRC'S SHARED "S" DRIVE
(OIG-18-A-06)

Attached is the Office of the Inspector General's (OIG) evaluation report titled *Evaluation of NRC's Shared "S" Drive*.

The report presents the results of the subject evaluation. Following the November 27, 2017, exit conference, agency 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. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

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

Office of the Inspector General

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

OIG-18-A-06
December 21, 2017

Results in Brief

Why We Did This Review

On July 6, 2017, OIG identified and accessed an employee's bank account information on a personal check that was scanned and saved to the agency's shared "S" drive.

After finding that the sensitive information was not protected by access controls, OIG reviewed the shared "S" drive for PII and identified a folder dated 2011, which had 35 subfolders for several offices in the agency. Of the 35 subfolders, 17 contained PII without appropriate access controls.

The objective was to assess how NRC effectively manages and protects Personally Identifiable Information (PII) stored on the shared "S" drive in accordance with Federal regulations.

Evaluation of NRC's Shared "S" Drive

What We Found

OIG evaluated NRC's shared drives to assess how the agency effectively manages and protects Personally Identifiable Information (PII) stored on the shared "S" drive in accordance with Federal regulations. OIG found weaknesses in the following areas:

- NRC staff store PII on the shared "S" drive without appropriate safeguards.
- NRC does not manage PII stored on the shared "S" drive.

What We Recommend

This report makes four recommendations to improve NRC's procedures and process for managing and protecting PII stored on the shared "S" drive.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

CD	Computer Drive
CSIRT	Computer Security Incident Response Team
EDO	Executive Director for Operations
IT	Information Technology
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
PII	Personally Identifiable Information
SUNSI	Sensitive Unclassified Nonsafeguards Information

I. BACKGROUND

The *Federal Privacy Act of 1974*, as amended (5 U.S.C. § 552a) (*Privacy Act*), establishes safeguards for the protection of records the Federal Government collects, maintains, uses, and disseminates on individuals. The *Privacy Act* is intended to balance the Government's need to maintain information about individuals with the rights of individuals to be protected against invasions of their privacy. The *Privacy Act* applies when information is retrieved by personal identifier from agency records (e.g., paper records, electronic records, and microfiche) that contain information about individuals. A personal identifier can include a person's name, social security number, and passport/visa number.

NRC defines PII as information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual. PII is a person's name in combination with any of the following information:

- driver's license number
- biometric record
- social security number
- bank account personal identifiable number or security code
- date or place of birth
- bank account number and credit card information
- medical or disability information
- mother's maiden name

PII is also a person's name in combination with any other information that would make the individual's personal identity easily traceable and available for unauthorized purposes.

NRC categorizes PII as sensitive unclassified nonsafeguards information (SUNSI). NRC defines SUNSI as any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC

and Federal programs, or the personal privacy of individuals. A need to know is required to access SUNSI.

NRC's Shared "S" Drive

A computer drive is a medium that is capable of storing and reading information and is not easily removed from a computer (like a CD, for example, which can be readily removed). NRC makes several computer network drives available to its employees for their daily work. These drives include a personal drive, an office shared drive, the read only drive and the agency shared "S" drive[1]. The shared "S" drive is best used to store "work in progress" documents that are readily accessible to NRC staff and contractors. NRC staff and contractors can save, edit, or delete documents stored on the agency's shared "S" drive.

At present, NRC has approximately 3,200 staff and 790 contractors who can access the agency's shared "S" drive. Storing information on the shared "S" drive means that any staff member or contractor with information technology (IT) access, who can connect to NRC's computer network, can also access any information stored on this drive. NRC prohibits staff and contractors from storing PII on the shared "S" drive without adding appropriate access controls.

On July 6, 2017, the Office of the Inspector General (OIG) identified and accessed PII stored on the NRC's shared "S" drive. OIG reported this incident to the Computer Security Incident Response Team (CSIRT), the Office of the Executive Director for Operations (EDO), and the Office of the Chief Information Officer (OCIO). NRC removed the folder from the shared "S" drive on August 16, 2017.

Recurring Problem of PII Protection on NRC's Shared "S" drive

OIG has conducted two reviews in the past that have identified issues with protection of PII. Specifically, OIG conducted the *Evaluation of Personal Privacy Information[2] found on NRC Network drive* (OIG-06-A-14), June 30,

[1]The "S" drive is a network storage location for files to be shared among multiple organizations and is also referred to as a shared drive. The "S" drive on each server can be accessed by all agency network users.
[2] Personal privacy information includes PII.

2006, and the *Audit of NRC's Shared "S" Drive* (OIG-11-A-15), July 27, 2011.

In OIG-06-A-14, OIG reported finding personal privacy information[3] on NRC's network drive because NRC staff did not follow existing guidance for protecting personal privacy information and lacked procedures for monitoring the NRC network drive for sensitive information.

Further, in OIG-11-A-15, OIG reported finding SUNSI, such as PII, and allegations material on the shared "S" network drive without appropriate access controls. This was a result of inadequate (1) training, (2) communication to NRC staff on specific practices, (3) guidance for protecting documents that contain SUNSI and are processed on the shared "S" network drive.

Federal Requirements and NRC's Responsible Offices

The National Institute of Standards and Technology (NIST) states the importance of protecting the confidentiality of PII in the context of information security. NIST provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII.

OCIO is responsible for managing NRC's information, employing information technology to enhance information access, and strengthening agency performance. Within OCIO, different branches are tasked with managing the agency's network. These branches include

- The *Information Security Planning and Oversight Branch,* which establishes and oversees the implementation of the agency's information security policies, procedures, and standards.

- The *Information Management Services Branch,* which ensures information management policy, standards, and governance are developed and followed based on applicable laws and regulations.

[3] OIG found personal privacy information on NRC's "R" drive. The read-only "R" drive is a network storage location for viewing files and documents. Users of this drive are restricted from editing documents and files stored on the drive.

- The *Service Delivery Management Branch,* which maintains the IT asset library and provides contract oversight.

- The *Network/Infrastructure Services Branch,* which manages the network and infrastructure.

II. OBJECTIVE

The objective was to assess how NRC effectively manages and protects Personally Identifiable Information (PII) stored on the shared "S" drive in accordance with Federal regulations.

III. FINDINGS

OIG's evaluation of NRC's shared "S" drive identified two opportunities for improvement on how NRC manages and protects PII stored on the shared "S" drive. Specifically, OIG found NRC staff store PII on the shared "S" drive without adding appropriate access controls and NRC does not review, delete or destroy PII stored on the shared "S" drive as needed. OIG makes four recommendations to improve NRC's management and protection of PII stored on the shared "S" drive.

A. NRC Staff Store PII on the Shared "S" Drive Without Appropriate Safeguards

NRC must ensure that personal data including PII is protected by reasonable security safeguards to mitigate such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. However, NRC staff store PII on the shared "S" drive without adding appropriate safeguards to the PII stored on the shared "S" drive. This occurs because NRC's policies and annual PII training do not provide specific guidance on how to effectively protect PII stored on the shared "S" drive. As a result, PII is at risk of being compromised.

What Is Required

Federal Guidance

NIST Special Publication 800-122 - *Guide to Protecting the Confidentiality of Personally Identifiable Information* requires agencies to ensure personal data is protected by reasonable security safeguards to mitigate such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists). For example, agencies can implement role-based access control, configuring it so that each user can only access the pieces of data necessary for the user's role. Another example is only permitting users to access PII through a control application that restricts access to PII, instead of permitting users to directly access the databases or files containing PII. Encryption of stored PII is another type of safeguard.

What We Found

NRC Staff Store PII on the Shared "S" Drive Without Appropriate Safeguards

NRC staff store PII on the shared "S" drive without using appropriate safeguards. On July 6, 2017, OIG identified and accessed an employee's bank account information on a personal check that was scanned and saved to the agency's shared "S" drive.

After finding that the sensitive information was not protected by access controls, OIG reviewed the shared "S" drive for PII and identified a folder dated 2011, which had 35 subfolders for several offices in the agency. Of the 35 office subfolders, 17 contained PII without appropriate access controls.

Why This Occurred

Insufficient Guidance and Training on Protecting PII

NRC's guidance and annual PII training do not provide specific procedures and training on how to effectively protect PII stored on the shared "S" drive. NRC's SUNSI handling requirements state that a need-to-know is required to access personal privacy information, which includes PII. In addition, NRC's Management Directive (MD) 12.6*, NRC's Sensitive Unclassified Information Security Program*, discusses safeguarding sensitive information.

Why This Is Important

In light of recent highly publicized government wide cyber security breaches, NRC as an organization, and NRC personnel need to protect PII stored on the shared "S" drive from unauthorized access. NRC needs to ensure that staff know, and have the proper training, policies and quality controls to protect PII from unauthorized access. In turn, NRC staff need to apply these training, policy and quality controls to protect PII stored on the shared "S" drive. PII stored on a shared "S" drive without safeguards may be vulnerable to unauthorized disclosure, thereby making individuals at risk of identity theft.

Recommendations

OIG recommends that the Executive Director for Operations

1. Revise NRC's SUNSI handling requirements guidance to specify how to effectively protect PII stored on the shared "S" drive.

2. Provide PII training annually to NRC staff on how to protect PII stored on the shared "S" drive.

B. NRC Does Not Manage PII Stored on the Shared "S" Drive

NRC management is required to review the agency shared "S" drive to identify and eliminate PII at least annually. However, NRC has not reviewed the shared "S" drive for PII since 2011 because NRC's management has not applied the necessary resources to perform this effort. As a result, PII may be at risk of unauthorized disclosure.

What Is Required

NRC's Yellow Announcement on PII

NRC's Yellow Announcement 096 – "*Guidance for Periodic Review of the Agency's Network Drive for the Presence of PII*", dated September 6, 2007, states that NRC's management will review the agency's shared "S" drive for the purposes of identifying and eliminating PII at least annually. It also states that in January of each year, NRC will search the shared "S" drive for files potentially containing PII.

What We Found

NRC Does Not Review the Shared "S" Drive for PII

NRC does not review the shared "S" drive for PII. This problem has been previously identified by OIG. As a result of OIG's *Evaluation of NRC Network Drive for Personal Privacy Information* (OIG-06-A-14), NRC directed offices and regions to review data generated and stored on the shared "S" drive for PII at least annually.

NRC began reviewing the shared "S" drive for PII in 2006 with a scanning tool, but stopped in 2011, reportedly due to inadequate resources and the amount of staff time associated with reviewing false positive results identified by the scanning tool. NRC stated that the scanning tool was difficult to use because it could not differentiate PII stored on the shared "S" drive from PII stored on other drives that had access controls in place. OIG was informed that NRC's periodic scans of the shared "S" drive were difficult to manage from a resource standpoint, given there were numerous false positives and the files were too large to review.

NRC Does Not Delete or Destroy PII as Required

NRC does not routinely remove PII as required. OIG found a folder dated 2011 of the network shared 'S' drive regarding information about the program offices. The scanned network drive results contained PII no longer used to conduct agency business.

NRC staff believe that the files and folders were restored to NRC's network after the November 2016 network interruption. During the restoration, some of the files and folders access permissions were not accurately set causing the potential inappropriate access of these files and folders.

In addition, OIG found a bank check and a bank statement, each dated 2010, which contained PII of an employee who no longer works at NRC. In this instance, the bank check and statement were no longer needed to conduct the agency business. An NRC official stated that it was not the

agency's responsibility to protect such information since the employee personally created the folder that contained the bank account details on the shared "S" drive.

Why This Occurred

NRC Management Has Not Applied the Necessary Resources to Review the Shared "S" Drive for PII

Since 2011, NRC management has not applied the necessary resources to review the shared "S" drive because it involves significant resources and coordination from program offices.

Why This Is Important

PII may be compromised and at risk of inappropriate disclosure. While OIG auditors found no evidence that the PII information had been compromised, NRC needs to protect the confidentiality, integrity, and reliability of PII required to fulfill the agency's mission.

Recommendations

OIG recommends that the Executive Director for Operations

3. Review the shared "S" drive for PII on a periodic timeframe.

4. Remove or delete PII from the shared "S" drive.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Revise NRC's SUNSI handling requirements guidance to specify how to effectively protect PII stored on the shared "S" drive.

2. Provide PII training annually to NRC staff on how to protect PII stored on the shared "S" drive.

3. Review the shared "S" drive for PII on a periodic timeframe.

4. Remove or delete PII from the shared "S" drive.

V. AGENCY COMMENTS

An exit conference was held with the agency on November 27, 2017. Agency management provided comments prior to and following this meeting, after reviewing a discussion draft. These comments are 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 assess how NRC effectively manages and protects Personally Identifiable Information (PII) stored on the shared "S" drive in accordance with Federal regulations.

Scope

The evaluation focused on reviewing NRC's shared "S" drive for PII and the requirements for protecting and managing PII stored on NRC's shared "S" drive. The evaluation was conducted at NRC headquarters from July 10, 2017, to September 25, 2017. Internal controls related to the evaluation's objective were reviewed and analyzed. Throughout the evaluation, OIG considered the possibility of fraud, waste, and abuse.

Methodology

OIG reviewed relevant Federal criteria for this evaluation, including the following:

- NIST requirements *Guide to Protecting the Confidentiality of Personally Identifiable Information*
- *National Archives General Records Schedule 4.2, Information Access and Protection Records*

OIG also reviewed NRC internal documents, including

- NRC Management Directive 3.2, "Privacy Act"
- NRC Management Directive 12.5, "NRC Cybersecurity Program"
- NRC Management Directive 12.6, "NRC Sensitive Unclassified Information Security Program"

- NRC's *Agency-Wide Rules of Behavior for Authorized Computer Use*.
- NRC's "The Right Tool for the Right Job: Navigating the NRC Intranet, SharePoint, Shared Drives and Agencywide Documents Access and Management System" December 2014
- NRC's Information and Records Management Guideline No 2016-07, *Cleaning Up Files on the "G" Drive and Network Shared Drive*
- Yellow Announcement 2008-063, "*NRC's Information Security and Records Management Requirements when Using Information Sharing and Learning Technologies such as SharePoint and Tomoye"*
- NRC's Comprehensive Records Disposition Schedule
- SUNSI Handling Requirements
- NRC Policy for Handling, Marking and Protecting SUNSI
- Yellow Announcement 2007-096, "*Guidance for Periodic Review of Agency Network Drives for the Presence of Personally Identifiable Information (PII)"*
- Yellow Announcement 2006-039, "*Safeguarding Personal Privacy Information"*

Additionally, OIG manually reviewed NRC's shared "S" drive for PII to assess if NRC staff manages and protects PII stored on the shared "S" drive in accordance with Federal regulations.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

The evaluation was conducted by Beth Serepca, Team Leader; Jaclyn Storch, Quality Assurance Manager; and Ebaide Esoimeme, Auditor.

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.