AUDIT REPORT

Audit of NRC's Shared "S" Drive

OIG-11-A-15 July 27, 2011

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

July 27, 2011

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S SHARED "S" DRIVE
(OIG-11-A-15)

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

The report presents the results of the subject audit. Informal comments provided by agency management and staff have been incorporated, as appropriate, into 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 audit. If you have any questions or comments about our report, please contact me at 415-5915 or Beth Serepca, Security and Information Team Leader, at 415-5911.

Attachment: As stated

Electronic Distribution

Edwin M. Hackett, Executive Director, Advisory Committee
on Reactor Safeguards
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety
and Licensing Board Panel
Stephen G. Burns, General Counsel
Brooke D. Poole, Director, Office of Commission Appellate Adjudication
James E. Dyer, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
R. William Borchardt, Executive Director for Operations
Michael F. Weber, Deputy Executive Director for Materials, Waste,
Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director
for Corporate Management, OEDO
Martin J. Virgilio, Deputy Executive Director for Reactor
and Preparedness Programs, OEDO
Nader L. Mamish, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Patrick D. Howard, Director, Computer Security Office
Roy P. Zimmerman, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials
and Environmental Management Programs
Cheryl L. McCrary, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
Miriam L. Cohen, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Catherine Haney, Director, Office of Nuclear Material Safety
and Safeguards
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
James T. Wiggins, Director, Office of Nuclear Security
and Incident Response
William M. Dean, Acting Regional Administrator, Region I
Victor M. McCree, Regional Administrator, Region II
Mark A. Satorius, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

EXECUTIVE SUMMARY

BACKGROUND

The President of the United States has directed Federal agencies to promote information sharing with the public and improve the transparency of Government operations.[1] Nevertheless, applicable laws and Governmentwide policies require the U.S. Nuclear Regulatory Commission (NRC) and other Federal agencies to protect some types of information against accidental or intentional disclosure.

NRC staff process on agency networks a category of sensitive unclassified information unique to NRC called Sensitive Unclassified Non-Safeguards[2] Information (SUNSI).[3] 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.

NRC staff can process electronic documents containing SUNSI in a variety of ways. For instance, some documents may be saved in the non-public version of NRC's online data system — the Agencywide Documents Access and Management System (ADAMS)[4]. Staff may also exchange documents on internal SharePoint[5] Web sites, which staff can configure to

[1] Office of Management and Budget Memorandum M-10-06; Subject: Open Government Directive; December 8, 2009.

[2] Safeguards information is information relating to certain material control and accounting procedures for special nuclear material or security measures for the physical protection of special nuclear material, source material, or byproduct material.

[3] NRC includes Personally Identifiable Information (PII) as a category of SUNSI. PII includes information that can be used to distinguish or trace an individual's identity, such as one's date of birth, Social Security Number, or home contact information.

[4] ADAMS is NRC's official repository for documents pertaining to the agency's regulatory activities.

[5] SharePoint is a software program that allows staff to set up Web sites to share information with others and allows staff to manage documents. SharePoint can be used to manage databases, reports, and business applications.

limit access rights to specific employees or groups of employees. Additionally, NRC staff can save documents on shared network drives.[6] These shared drives include "G" drives accessible by staff within NRC program offices; an "R" drive, an agencywide drive with read-only access; and an "S" drive, which allows all staff, whose user accounts are on the same file server, to add, read, edit, and delete documents unless documents are stored in folders configured to limit access to specific employees or groups of employees. Regardless of how NRC employees exchange SUNSI on agency networks, Federal law requires that NRC maintain adequate controls over the confidentiality, integrity, and availability of this information.[7]

PURPOSE

The audit objective was to assess whether NRC effectively protects electronic documents containing Personally Identifiable Information (PII) and other types of SUNSI on NRC's shared network drives.

RESULTS IN BRIEF

NRC has policies for protecting electronic documents containing SUNSI that are processed on agency shared network drives. Nevertheless, NRC can improve training, communication, coordination, and quality assurance controls to ensure that access to these documents is limited to a need-to-know basis. NRC guidance requires that access to documents containing SUNSI be controlled on a need-to-know basis. NRC has procedures to control documents containing SUNSI that are stored on its computer network. Nevertheless, auditors found documents containing specific types of SUNSI, such as PII and allegations material, on shared network drives without appropriate protections.

[6] Documents containing classified or Safeguards information may not be processed on NRC's unclassified networks or placed in ADAMS.

[7] Federal Information Security Management Act of 2002, 44 U.S.C § 3542.

RECOMMENDATIONS

This report makes recommendations to improve training, communication, coordination, and quality assurance controls to ensure SUNSI is limited to a need-to-know basis.

AGENCY COMMENTS

At an exit conference on June 30, 2011, agency management provided informal comments on a draft of this report. The Office of the Inspector General incorporated some of these comments as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

ABBREVIATIONS AND ACRONYMS

ADAMS	Agencywide Documents Access and Management System
CSO	Computer Security Office
CUI	Controlled Unclassified Information
IT	information technology
NARA	U.S. National Archives and Records Administration
NRC	U.S. Nuclear Regulatory Commission
OIG	Office of the Inspector General
OIS	Office of Information Services
PII	Personally Identifiable Information
SBU	Sensitive but Unclassified
SUNSI	Sensitive Unclassified Non-Safeguards Information

TABLE OF CONTENTS

BACKGROUND

The President of the United States has directed Federal agencies to promote information sharing with the public and improve the transparency of Government operations.[8] Nevertheless, applicable laws and Governmentwide policies require NRC and other Federal agencies to protect some types of information against accidental or intentional disclosure. For example, the Federal Government has in recent years increased its emphasis on protecting Personally Identifiable Information (PII) processed on its computer networks. PII includes information that can be used to distinguish or trace an individual's identity, such as one's date of birth, Social Security Number, or home contact information. NRC processes some PII in dedicated record systems to comply with the Privacy Act of 1974.[9] However, not all PII is subject to Privacy Act protections and may be processed on the agency's shared network drives. Given the sensitivity of this information, NRC has specific policies that agency staff must follow in storing and transmitting PII electronically. Further, NRC has a formal process for documenting potential PII breaches, reporting these incidents to the Department of Homeland Security,[10] and taking remedial action if necessary. As an additional precaution, NRC staff perform annual automated scans of the agency's networks to detect PII that may be stored without adequate protections. Positive results of these scans are reported to program office staff, who then determine the proper course of action on a case-by-case basis.

NRC staff also process on agency networks a broader category of sensitive unclassified information unique to NRC called Sensitive Unclassified Non-Safeguards[11] Information (SUNSI).[12] NRC defines SUNSI as:

[8] Office of Management and Budget Memorandum M-10-06; Subject: Open Government Directive; December 8, 2009.

[9] NRC's Privacy Act systems of records are documented in the Federal Register, and include records such as personnel performance appraisals, payroll accounting records, personnel security files, and drug testing program records.

[10] Specifically, NRC must report a potential PII breach to the Department of Homeland Security's United States Computer Emergency Response Team within one hour of discovering the breach.

[11] Safeguards information is information relating to certain material control and accounting procedures for special nuclear material or security measures for the physical protection of special nuclear material, source material, or byproduct material.

> …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.

In general, SUNSI is information pertaining to agency operations that should be exchanged only on a need-to-know basis. Further, SUNSI must not be made publicly available without formal internal review for decontrol, or review in response to Freedom of Information Act requests for particular documents. NRC divides SUNSI into the following seven main categories:

1. Allegation information.
2. Investigation information.
3. Security-related information.
4. Proprietary information.
5. Privacy Act information/PII.
6. Federal-, State-, foreign government-, and international agency-controlled information.
7. Sensitive internal information.

The U.S. National Archives and Records Administration (NARA) is currently leading a Governmentwide initiative to create a primary sensitive information category called "Controlled Unclassified Information" (CUI)[13] that will include many subcategories that Federal agencies may assign to their CUI documents. Once CUI becomes standardized across the Federal Government, it will supersede SUNSI at NRC. As a result, NRC has developed a set of common document categories and related markings that include the SUNSI categories. NRC has submitted this information to NARA for review and inclusion in the CUI program.

NRC staff can process electronic documents containing SUNSI in a variety of ways. For instance, some documents may be saved in the non-public version of NRC's Agencywide Documents Access and Management

[12] NRC includes PII as a category of SUNSI information.

[13] Executive Order No. 13556 of November 4, 2010.

System (ADAMS)[14] data system. Staff may also exchange documents on internal SharePoint[15] Web sites, which staff can configure to limit access rights to specific employees or groups of employees. Additionally, NRC staff can save documents on shared network drives.[16] These shared drives include "G" drives accessible by staff within NRC program offices; an "R" drive, an agencywide drive with read-only access; and an "S" drive, which allows all staff, whose user accounts are on the same file server, to add, read, edit, and delete documents unless documents are stored in folders configured to limit access to specific employees or groups of employees. Regardless of how NRC employees exchange SUNSI on agency networks, Federal law requires that NRC maintain adequate controls over the confidentiality, integrity, and availability of this information.[17]

NRC's network drives reside on servers located at NRC headquarters, regional offices, and the Technical Training Center. In 2010, NRC completed a process of consolidating its servers in an effort to make more efficient use of its information technology (IT) infrastructure. As part of the process, NRC decommissioned existing servers, and installed new servers from the same vendor product line that supports the agency's e-mail, Web-based applications, and other IT functions. NRC also transferred data from outgoing servers to new servers and reconfigured connections among various drives to replicate connections that existed before the consolidation process began. This affected the labeling and layout of drives seen by staff on their computer screens. For example, multiple "R" and "S" drives were consolidated into single "R" and "S" drives.

NRC's Office of Information Services (OIS) manages the agency's IT infrastructure and oversees network upgrades, such as server consolidation performed by contractors. OIS also organizes and conducts NRC's annual PII scans. IT coordinators designated by NRC program

[14] ADAMS is NRC's official repository for documents pertaining to the agency's regulatory activities.

[15] SharePoint is a software program that allows staff to set up Web sites to share information with others and allows staff to manage documents. SharePoint can be used to manage databases, reports, and business applications.

[16] Documents containing classified or Safeguards information may not be processed on NRC's unclassified networks or placed in ADAMS.

[17] Federal Information Security Management Act of 2002, 44 U.S.C § 3542.

offices coordinate within their respective offices reviews of PII scan results. These IT coordinators also facilitate IT service requests on behalf of staff in their respective program offices. In addition, NRC’s Computer Security Office (CSO) plays a primary role in detecting, analyzing and responding to information security breaches, as well as developing and implementing NRC’s IT security policies.

II. PURPOSE

The audit objective was to assess whether NRC effectively protects electronic documents containing PII and other types of SUNSI on NRC’s shared network drives. This audit did not address protection of documents containing classified and Safeguards information. The report appendix contains information on the audit scope and methodology.

III. FINDING

NRC Can Improve Training, Communication, Coordination, and Quality Assurance Controls to Ensure Security of SUNSI on Network Drives

NRC has policies for protecting electronic documents containing SUNSI that are processed on agency shared network drives. Nevertheless, NRC can improve training, communication, coordination, and quality assurance controls to ensure that access to these documents is limited to a need-to-know basis. NRC guidance requires that access to documents containing SUNSI be controlled on a need-to-know basis. NRC has procedures to control documents containing SUNSI that are stored on its computer network. Nevertheless, auditors found documents containing specific types of SUNSI, such as PII and allegations material, on shared network drives without appropriate protections. The problems occurred for four main reasons.

1. NRC has not provided adequate training on specific practices for protecting documents containing SUNSI that are processed on shared network drives.

2. NRC has not adequately communicated to its staff specific guidance for protecting documents containing SUNSI that are processed on network shared drives.

3. There are a range of skills among IT coordinators, but NRC does not provide them with role-based training regarding NRC network and information security policies. This constrains IT coordinators from being able to provide guidance consistently on how to protect SUNSI stored on NRC's shared network drives and ensure compliance with NRC policy.

4. Recent technology upgrades resulted in a temporary loss of access controls over information on the "S" drive.

Although auditors found no evidence that SUNSI identified on shared network drives had been compromised, these issues require management attention so that NRC can better manage risks to the confidentiality, integrity, and reliability of SUNSI processed on the agency's shared network drives.

SUNSI Should Be Accessible Only on a "Need-to-Know" Basis

NRC Management Directives[18] and other internal guidance[19] state that NRC staff who have a need to know sensitive information to perform their official duties may have access to that information; otherwise, access should be restricted. NRC provides instructions on how to implement access controls on all categories of SUNSI within ADAMS.[20] For example, "allegation information" may not be processed in ADAMS, while "security-related information" may be processed in ADAMS but must have assigned access rights to user groups with a need to access the information to perform their official duties. This guidance also describes how to transmit SUNSI, including PII, within and outside NRC.

[18] Management Directive 12.5, *NRC Automated Information Security Program,* and Management Directive 12.6, *NRC Sensitive Unclassified Information Security Program.*

[19] NRC posts information about SUNSI policies and procedures on the agency's intranet.

[20] ADAMS has a publicly available version, as well as a non-public version restricted to employees with network access.

Auditors Found Instances of SUNSI, Including PII, on Shared Network Drives

Office of the Inspector General (OIG) auditors systematically reviewed documentation stored on the agency's "S" drive and found documents containing all categories of SUNSI, including PII. Examples of PII found include the personal information of past and current NRC commissioners, including home addresses, home telephone numbers, passport information, and credit card information.[21] PII was found despite NRC's efforts to locate all PII in its annual automated scans as recommended by the OIG in 2006.[22] Table 1 shows examples of SUNSI that auditors found in their review of "S" drive documentation.

[21] Some of the PII that auditors found was embedded in portable document format files, or "PDF files," which can contain images. NRC's annual PII scan of shared network drives did not detect these files.

[22] OIG-06-A14, *Evaluation of Personal Privacy Information Found on NRC Network Drives*.

Table 1: Examples of SUNSI Including PII Detected on "S" Drive

Information Category	Sub-Definition	Example(s) Found on "S" Drive
Personally Identifiable Information	All information that can be used to distinguish or trace an individual's identity.	A Commissioner's and employees' home addresses, home phone numbers, passport images, and credit card images; an employee's personal bank account information; and personnel action documents.
Allegation Information	Confidential or sensitive allegation information.	Allegation intake forms with names of accused individuals, accusations against the individuals, and a notice of violation issued as a result of an allegation.
Security-Related Information	10 CFR 2.390 Information, information that could be useful to a terrorist attack, sensitive Homeland Security information, licensee submitted critical energy infrastructure or Transportation Security Administration information.	Multiple files and folders filled with information categorized as "Security-Related Information," including requests for information and letters, information on security of fuel cycle facilities, and cybersecurity program information for nuclear facilities.
Sensitive Internal Information	Attorney client privilege, attorney work product, pre-decisional information, information submitted to the Commission marked "Sensitive," and others.	More than 50 folders containing legal advice and including names and details of advice sought.
Investigation Information	Any Office of Investigations or Office of the Inspector General investigation related documents.	Report of an Office of Investigations case.
Federal-, State-, Foreign Government, and International Agency Controlled Information	Information not to be released to foreign nationals, Official Use Only Department of Energy information, Naval Nuclear Propulsion Information, Sensitive but Unclassified (SBU) from Department of State, and others.	Foreign travel trip reports, SBU letters.
Proprietary Information	Trade Secrets, confidential commercial or financial information, Institute of Nuclear Power Operations, Source Evaluation Proprietary Data.	Multiple IT system management documents, including test plans and other proprietary data.

Additionally, during the course of this audit, access control profiles for allegations folders on a regional office shared network drive changed temporarily to a general default setting.[23] This error occurred during a network upgrade and, temporarily, made the allegations folders accessible to any employees with regional office network access, regardless of their need to know this information. Upon detecting this error, NRC staff referred the error to OIS and CSO, and the original access permissions—which limited folder access to three NRC employees—were restored.

Training, Communication, Coordination, and Technological Factors Contributed to Improper Handling of SUNSI on NRC Networks

The discovery of SUNSI on shared network drives and the release of allegations data in a regional office occurred for four main reasons:

1. NRC has not provided adequate training to NRC staff on specific practices for protecting documents containing SUNSI that are processed on shared network drives. Although IT coordinators stated that NRC users receive annual training, the annual online training classes offered by the NRC address broader computer and information security issues. For example, the annual Information Security Awareness course focuses largely on protection of classified[24] and Safeguards information, and does not address protection of SUNSI stored electronically on agency shared network drives. NRC's annual Computer Security Awareness course addresses PII protections, but not NRC-specific policies and procedures for protecting SUNSI.[25] Additionally, existing PII training does not include knowledge checks, such as multiple choice questions, and briefly mentions in a single bullet point that staff should not store PII on the agency's shared network drives.

[23] The correct access control profiles limited folder access to just three NRC regional office staff.

[24] Classified information is information that could cause damage to national security as a result of unauthorized disclosure.

[25] This training advises staff to store "sensitive information, including PII" only on "an authorized information system." It also advises staff never to transmit, store or process this information on a "non-senstive system."

2. NRC has not adequately communicated to its staff specific guidance for protecting documents containing SUNSI that are processed on shared network drives. NRC has issued network announcements regarding SUNSI and PII-specific policies. However, these e-mail announcements—if opened and read by NRC staff—often require staff to follow Intranet links to more detailed discussion of agency policy. In addition, network announcements with detailed instructions for staff are not always timed closely with network changes that could impact SUNSI protection. For example, in December 2010, NRC sent an announcement about changes to network shared drives,[26] which advised staff to "be prudent" about information saved on these drives. In May 2011—five months later—NRC sent a more detailed announcement about protecting PII on shared network drives through access control settings.

3. Varying skill levels and the limited scope of IT coordinators' duties constrain their ability to educate staff about policies for handling SUNSI and ensure staff compliance. In one quarter of the 28 IT coordinator interviews, [27] IT coordinators were uncertain whether NRC staff used the agencywide shared "S" drive, and whether it was needed to perform business, thus suggesting a lack of knowledge on where their office's data is processed, stored, or shared. Additionally, IT coordinators' formal roles and responsibilities are limited to facilitating IT service requests on behalf of staff. However, auditors found that IT coordinators interact with their customers on network and information security issues—most notably, through their work on annual PII scans—but do not receive role-based training that reflects this work.

4. In December of 2010, a network upgrade temporarily removed access control profiles on a limited number of allegations files. NRC staff who use the files reported this error, and corrective action was taken. Although this was an isolated incident, NRC staff acknowledged a need for quality assurance checks after contractors perform network upgrades to ensure access controls are maintained.

[26] The "R" and "S" drives, specifically.

[27] NRC has IT coordinators who support 31 offices including the regions. Some provide agencywide support. Each office may have one or up to nine IT coordinators.

Management Attention Is Needed To Control Risk of Disclosure, Modification, or Deletion of SUNSI

Despite instances of problems with controls over SUNSI stored on NRC shared network drives uncovered by the OIG, auditors found no evidence suggesting that this information had been compromised. Nevertheless, without proper training, policy communication, IT coordinator support, and quality assurance controls, SUNSI on the shared network drives may be at greater risk of unintentional or intentional disclosure, modification, and/or deletion. This, in turn, could compromise the confidentiality, integrity, and reliability of SUNSI that NRC needs to perform its mission and protect the privacy of agency staff and public stakeholders. Management attention is needed to improve security of SUNSI stored on NRC's networks, and reduce the risk of information security breaches that could compromise agency operations and the privacy of its personnel.

IV. RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Revise current PII training to include practical scenarios and knowledge checks that address processing PII on shared network drives.

2. Revise current information security training for NRC staff to address specific practices for protecting SUNSI on the agency's shared network drives.

3. Develop CUI policies and guidance for storing and protecting CUI in agency shared drives, and:
   a. post this guidance on the NRC intranet; and
   b. include this guidance in annual training.

4. Provide IT coordinators with role-based training focusing on NRC information and network security policies, and means for ensuring staff compliance with these policies.

5. Implement procedures for quality assurance checks following network upgrades to ensure that access controls are preserved in

shared network drives that process documents containing SUNSI/CUI.

V. AGENCY COMMENTS

At an exit conference on June 30, 2011, agency management provided informal comments on a draft of this report. The Office of the Inspector General incorporated some of these comments as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

Appendix

*S*COPE AND METHODOLOGY

The audit objective was to assess whether NRC effectively protects electronic documents containing PII and other types of SUNSI on NRC's shared network drives. To address the audit objective, OIG auditors conducted multiple interviews of NRC staff representing OIS and CSO. Auditors also conducted 28 interviews with IT coordinators representing most NRC program and regional offices. At the time of our analysis, OIS listed 92 IT coordinators representing 31 headquarters and regional offices. OIG auditors also systematically examined files on the agency's "S" drive to determine whether SUNSI, including PII, was saved inappropriately.

OIG auditors reviewed pertinent NRC and Federal Government guidance, including:

- NRC SUNSI Handling Requirements.
- MD 12.6, *NRC Sensitive Unclassified Information Security Information Program.*
- MD 12.5, *NRC Automated Information Security Program.*
- NIST Special Publication 800-53.
- NIST Special Publication 800-60.

OIG auditors also reviewed the content of the three required information security annual training online classes – Computer Security Awareness , Personally Identifiable Information, and Information Security Awareness – for content on SUNSI handling.

OIG conducted this performance audit, from January 2011 through May 2011, at NRC headquarters in Rockville, Maryland, in accordance with generally accepted Government auditing standards. Those standards require the audit to be planned and performed with the objective of obtaining sufficient, appropriate evidence to provide a reasonable basis for any findings and conclusions based on the stated audit objective. OIG believes that the evidence obtained provides a reasonable basis for the report findings and conclusions based on the audit objective. OIG reviewed and analyzed internal controls related to the audit objective. Throughout the audit, auditors were aware of the possibility of fraud, waste, or misuse in the program. The audit was conducted by Beth

Serepca, Team Leader; Paul Rades, Audit Manager; Melissa Schermerhorn, Senior Analyst; and Gail Butler, Analyst.