AUDIT REPORT

Audit of NRC's Safeguards Information Local Area Network and Electronic Safe

OIG-13-A-16 April 1, 2013

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

April 1, 2013

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S SAFEGUARDS INFORMATION LOCAL AREA NETWORK AND ELECTRONIC SAFE (OIG-13-A-16)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of NRC's Safeguards Information Local Area Network and Electronic Safe.*

The report presents the results of the subject audit. Agency comments provided at the March 20, 2013, exit conference 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 follow-up 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, Team Leader, Security and Information Management Team, at 415-5911.

Attachment: As stated

EXECUTIVE SUMMARY

BACKGROUND

The U.S. Nuclear Regulatory Commission (NRC) developed its Safeguards Information Local Area Network and Electronic Safe (SLES) system to store and manage electronic Safeguards Information (SGI) documents.

SLES features two distinct components: a secure wireless Local Area Network (LAN) and an electronic safe (E-Safe) for SGI documents. The SGI LAN component is a network with a secure architecture and is dedicated for use in SGI data processing. The E-Safe component is a secure electronic data repository for SGI records. E-Safe users are able to create, capture, search, and retrieve data from this repository. The adoption of these various techniques into SGI operations was intended to ensure that E-Safe will contain all SGI created or received by NRC, thereby eliminating the need to maintain separate, individual collections of SGI.

OBJECTIVE

The audit objective was to determine if SLES meets its operational capabilities and applicable security controls.

RESULTS IN BRIEF

NRC has developed a secure electronic system to store SGI while also reducing paper SGI and the space needed to store SGI documents; however, opportunities exist for improvement. Specifically, the system (A) does not fully meet user needs and (B) uses inconsistent access rights.

RECOMMENDATIONS

This report makes recommendations to improve the agency's SLES system. A list of these recommendations appears on page 21 of this report.

AGENCY COMMENTS

At an exit conference on March 20, 2013, agency management stated their agreement with the findings and recommendations in this report. Agency management also provided supplemental information that has been incorporated into this report, as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

ABBREVIATIONS AND ACRONYMS

CFR – Code of Federal Regulations

CD – Compact Disc

DVD – Digital Versatile Disc

E-Safe – Electronic Safe

HSPD-12 – Homeland Security Presidential Directive 12

IT – Information Technology

LAN – Local Area Network

NRC – U.S. Nuclear Regulatory Commission

NSIR – Office of Nuclear Security and Incident Response

OIG – Office of the Inspector General

OIS – Office of Information Services

SGI – Safeguards Information

SLES – Safeguards Information Local Area Network and Electronic Safe

TABLE OF CONTENTS

I. BACKGROUND

SLES Overview

The U.S. Nuclear Regulatory Commission (NRC) developed its Safeguards Information Local Area Network and Electronic Safe (SLES) system to store and manage electronic Safeguards Information (SGI)[1] documents. SLES was created in response to the Commission's January 2004 directive[2] that staff "develop and implement a secure intranet capability that allows appropriate NRC staff to share safeguards and classified information[3] internally in a secure and effective manner."

SLES was created to meet the following business needs:

- Provide a secure network for authorized users to access SGI documents electronically.
- Reduce the volume of SGI document storage space.
- Act as a secure SGI records repository in compliance with National Archives and Records Administration requirements.
- Enable record and document management (i.e., add, store, search, retrieve, collaborate, and disposition) of SGI in a centralized electronic document management system.

Prior to SLES, SGI was generated and maintained by NRC employees who were authorized as SGI custodians. These custodians used secure safes to control the information and ensure protection from unauthorized disclosure. While some electronic files were stored on compact discs (CD) and removable hard disks, most of the SGI documents were in paper (hardcopy) format. Regardless of format, SGI was stored in either lock bar cabinets or safes.[4] Over time, managing SGI hardcopy, individual CDs, and files on removable hard disks in the secure lock bar cabinets

[1] SGI is a special category of sensitive unclassified information to be protected as authorized by Section 147 of the Atomic Energy Act. SGI concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material. While SGI is considered sensitive unclassified information, its handling and protection more closely resembles the handling of classified confidential information than other sensitive unclassified information.
[2] Staff Requirements Memorandum M040114A, "Briefing on the Status of OCIO Programs, Performance, and Plans," dated January 30, 2004.
[3] Only SGI is stored in SLES; NRC does not have an electronic system for storing classified information.
[4] Lock bar cabinets are steel file cabinets with a combination lock that secures all of the file drawers. Paper SGI is required to be stored in lock bar cabinets but may also be stored in safes with classified information.

had become increasingly difficult, which caused delays in locating, accessing, and sharing SGI with authorized staff. This led to NRC's development and implementation of a secure intranet capability that would allow authorized NRC staff in the headquarters and regional offices to share SGI in a secure and effective manner.

The Office of Nuclear Security and Incident Response (NSIR) began using SLES in 2008. In 2009, NRC validated the SLES architecture to ensure the scalability and security of the system prior to its deployment agencywide. SLES officially went "live" at NRC headquarters in January 2010, and then on a staggered basis to the NRC regional offices and resident inspector sites, with full implementation by May 2012.

SLES Features

SLES features two distinct components: a secure wireless Local Area Network (LAN) and an electronic safe (E-Safe) for SGI documents. The SGI LAN component is a network with a secure architecture and is dedicated for use in SGI data processing. The SGI LAN essentially provides access to E-Safe via kiosk workstations, desktop terminals, or laptops.[5] The E-Safe component is a secure electronic data repository for SGI records. E-Safe users are able to create, capture, search, and retrieve data from this repository. Records are captured in E-Safe through scanning paper copies, uploading documents from CDs and Digital Versatile Discs (DVD), and creating documents within the system itself. The adoption of these various techniques into SGI operations was intended to ensure that E-Safe will contain all SGI created or received by NRC, thereby eliminating the need to maintain separate, individual collections of SGI.

E-Safe stores all SGI documents in "locked" electronic folders. NRC employees must follow a multistep process to obtain access to these folders and documents. First, the employee must create an SLES user account by submitting a form to the SLES help desk. Next, the employee's branch chief must email the SLES help desk to specify which

[5] There are three different ways to access SLES depending on the user. Most users will access SLES via one or two shared kiosk workstations within an office. Frequent SLES users may have their own SLES desktop computer terminal. Finally, resident inspectors located at nuclear power plant sites are provided an SLES laptop.

documents the employee should be authorized to read. This authorization serves as the "need-to-know."[6] Finally, the SLES help desk assigns the employee to one or more user groups[7] that have the ability to read those documents.

SLES also provides features that do not involve E-Safe. The system contains electronic collaboration rooms where users can develop and edit SGI documents in a secure and protected environment, and it has a secure email function where users can email SGI documents using approved encryption protocols.

SLES Security

The SLES LAN is isolated from the NRC LAN, Internet, and all other networks to enhance security and prevent migration of SGI data off the SLES system. The system uses Virtual Private Network technology to ensure secure encrypted connections between remote locations. Security is further enhanced by using multi-factor authentication. Authenticating to SLES is done through an individual's Personal Identity Verification card,[8] which extends security to SLES through a well-established, organization-wide identity verification infrastructure. Further, to access the E-Safe component of SLES, users must have an additional user identification and password.

The SLES system is designed to provide data protection and availability through regular periodic server file backups and through a redundant secondary ("failover") system at NRC's Region IV office location. The purpose of the failover system is to ensure that the SLES system can remain available to users and that data would not be lost in the event that the primary system at NRC headquarters becomes nonfunctional. The failover site houses a duplicate set of servers that contain a mirror image of the primary site data servers. In an event where the headquarters site

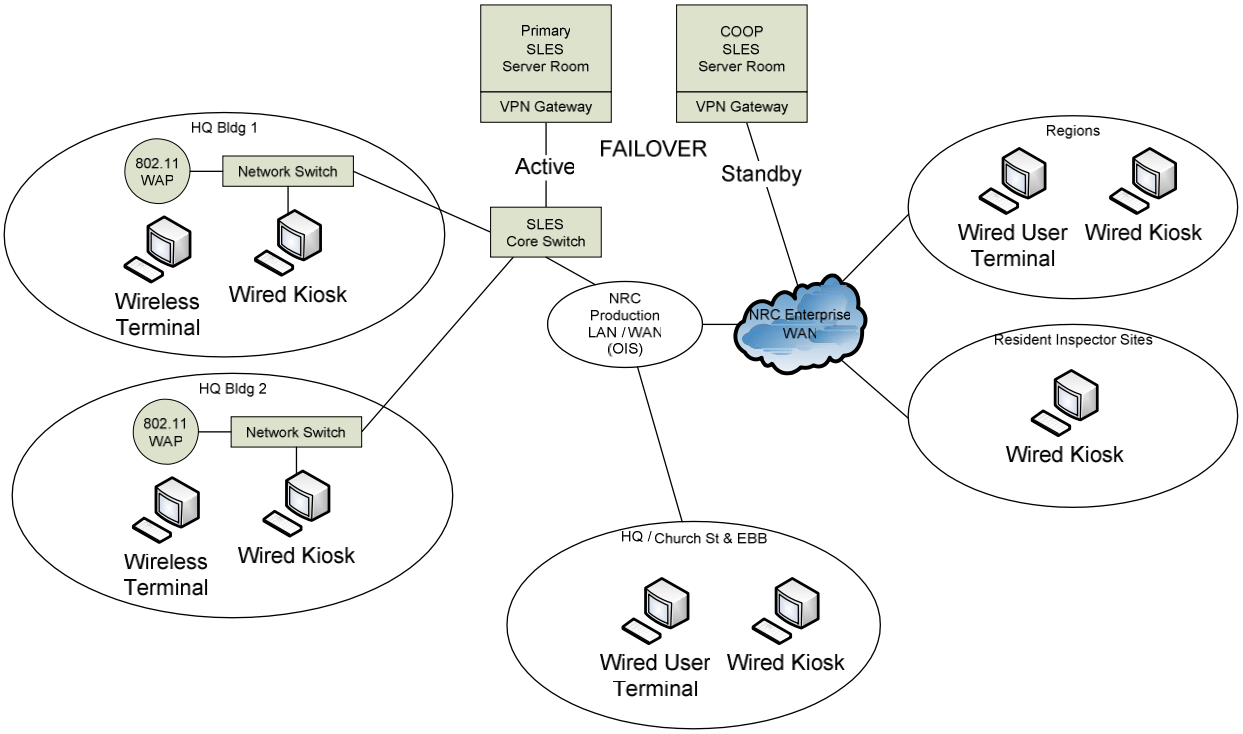
[6] *"Need-to-know"* means a determination by a person having responsibility for protecting SGI that a proposed recipient's access to SGI is necessary in the performance of official, contractual, licensee, applicant, or certificate holder employment.

[7] All user groups are assigned to specific folders that contain SGI documents. Users assigned to a user group get access rights to all folders and documents assigned to that user group.

[8] On August 27, 2004, President George W. Bush signed Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors." HSPD-12 directed the implementation of a new standardized badging process, which was designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued Government identification.

is not available for the system users, the secondary site would become the primary. See Figure 1 for a depiction of the SLES network topology map.[9]

Figure 1: SLES Network Topology Map



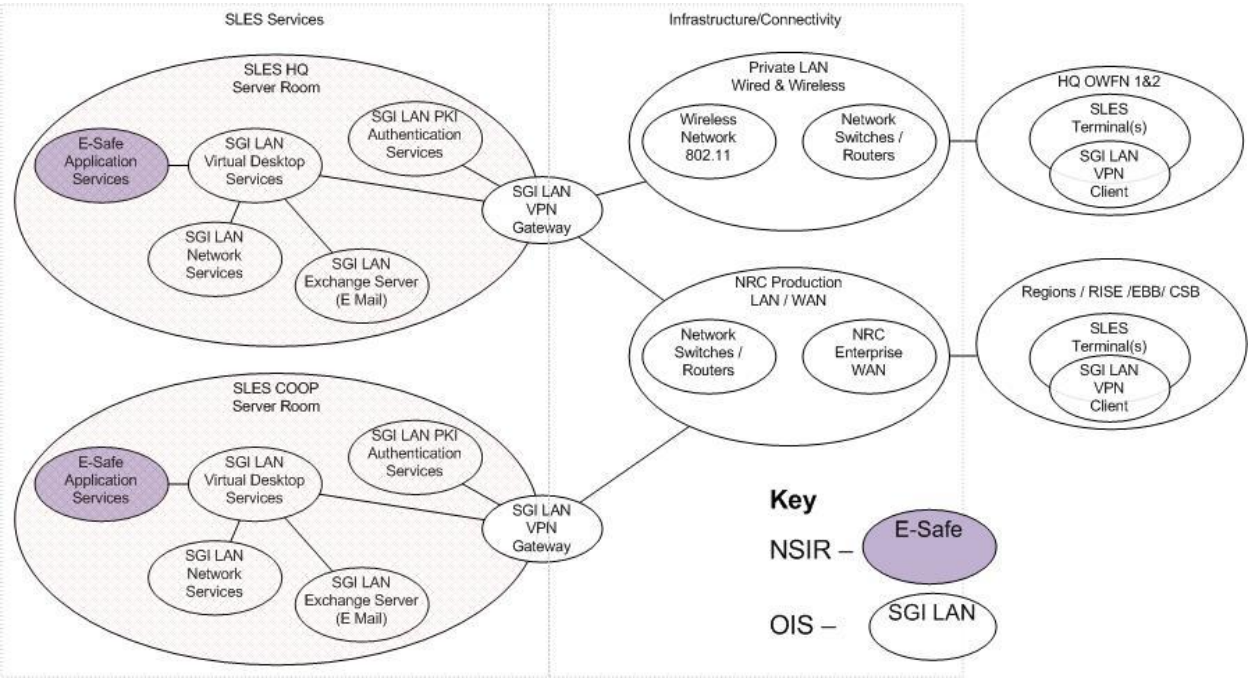
Source: NRC

[9] The failover site is depicted by the green box labeled "COOP SLES Server Room."

Program Offices

On October 1, 2011, NRC transitioned ownership of the SLES system from NSIR to the Office of Information Services (OIS). Under this arrangement, OIS manages the entire hardware infrastructure and tasks associated with the system's operating maintenance for the secure LAN and application. OIS is also responsible for project management, help desk support, system operations, and maintenance of SLES. NSIR, the creator and original SLES system owner, manages the E-Safe software application that is hosted on the servers maintained by OIS. NSIR handles E-Safe issues dealing with the system's business process, for example, adding users to the application, maintaining records taxonomy, and giving permission to access SGI folders or documents. NSIR is essentially responsible for the SGI data within SLES.[10] See Figure 2 for more information on OIS and NSIR SLES roles and responsibilities.

Figure 2: OIS and NSIR SLES Roles and Responsibilities



Source: NRC

[10] It should be noted that the SGI data is not owned by the SLES system or NSIR, but rather by the respective departments/authors that it came from.

Program Resources and Costs

NRC receives SLES support from a nine-member contractor team[11] under a single contract for two types of services: (1) Operations and Maintenance and (2) Records Management. After the system ownership transition from NSIR to OIS, OIS assumed the Operations and Maintenance (help desk and operations) responsibility from NSIR while NSIR maintained control of the Records Management (paper SGI scanning into SLES) portion. OIS has committed .33 full-time equivalent personnel to SLES; NSIR removed all full-time equivalent personnel from SLES after it transitioned system ownership to OIS in 2011.

NRC paid approximately $5.3 million to develop SLES and pays approximately $1.2 million annually for its SLES contract. Of this amount, roughly $831,000 goes to the support contractor, $315,000 is applied to software, and $78,000 is targeted for hardware.

[11] The contractor team consists of seven full-time and two part-time members.

II. OBJECTIVE

The audit objective was to determine if SLES meets its operational capabilities and applicable security controls. The report appendix contains information on the audit scope and methodology.

III. FINDINGS

NRC has developed a secure electronic system to store SGI while also reducing paper SGI and the space needed to store SGI documents; however, opportunities exist for improvement. Specifically, the system (A) does not fully meet user needs and (B) uses inconsistent access rights.

A. SLES Does Not Fully Meet User Needs

Information Technology (IT) Systems should improve agency productivity and efficiency while reducing paper.[12] SLES was created to allow NRC staff to share SGI in a secure and effective manner. However, SLES does not fully meet user needs, and while it has reduced the amount of SGI paper documents maintained by NRC offices, a significant amount still remains. This has occurred because NRC management has not given SLES high priority, specifically:

- There is no single individual who serves as a business "champion"[13] for integrating SLES into the NRC business process.
- NRC lacks adequate communication channels to discuss system issues between SLES staff and its users.

As a result, the system is not being used to its potential and more resources must be used to maintain paper SGI records, possibly resulting in fiscal waste.

Information Technology Systems Should Improve Productivity and Efficiency While Reducing Paper

IT Systems should improve agency productivity and efficiency while reducing paper. The Paperwork Reduction Act of 1995 states that Federal agencies should ensure that IT is acquired, used, and managed to improve performance of agency missions. The act also promotes the use of IT by agencies to improve the productivity, efficiency, and effectiveness of agency programs. Finally, it states that agencies should minimize the cost of the creation, collection, maintenance, use, and dissemination of information, including the use of technology to reduce information collection burdens.

According to an NRC Staff Requirements Memorandum from January 2004, the Commission directed that staff "develop and implement a secure intranet capability that allows appropriate NRC staff to share safeguards and classified information internally in a secure and effective manner."

[12] Paperwork Reduction Act of 1995.
[13] A champion is a person who voluntarily works to facilitate the adoption, implementation, and success of a cause, policy, program, project, or product.

SLES Is Not Meeting User Needs and a Large Amount of Paper SGI Still Remains

SLES does not fully meet user needs. Based on interviews with 26 active SLES users, auditors identified the following common themes:

- SLES official folder and document organization is confusing and not intuitive – Fourteen users commented that finding documents in the system is difficult or that the folder and document organization within SLES is poorly organized and categorized. Users have remarked that unless they know the NS number[14] of the document they are looking for, they may not be able to locate the documents within SLES. Moreover, many of the folders in SLES are empty. The Office of the Inspector General (OIG) reviewed 492 folders of the 5,699 folders within SLES, and found that 55 percent (272 folders) of the folders reviewed contained no documents at all.

- The search function is poor as it is limited to "read" permission only – SLES is arranged so that users with only "browse" permission cannot see any results (document titles) when conducting a formal search through the SLES search engine.[15] To see results when conducting formal document searches, users must have read permission.[16] This is a problem because the default setting for all SLES users is set at browse permission, and even for those users with read permission, search results can still be extremely limited because users can only see search results to folders *for which they have read permission*.

  For example, if users had read permission to a folder containing Beaver Valley security information, the users would be able to search for any documents in the Beaver Valley folder and view all

[14] An NS number is a specific number assigned to every document in SLES, similar to the ML number in NRC's Agencywide Documents Access and Management System (ADAMS).
[15] If users have "browse" permission, they are able to see document titles only if they manually scroll through the entire inventory of SLES documents. Users with browse permission cannot do an actual search to identify a particular document.
[16] Permissions control what a user can do. Examples of SLES permissions include browse, read, and edit. Browse, the default user permission, simply allows users to scroll through SLES and view folder and document titles; read allows users to open and read the contents of all documents within a folder; and edit allows users to edit documents. Users must first obtain the need-to-know prior to receiving read or edit permissions.

of the results. But if the same users needed information located in another folder where they only had the default browse permission (e.g., Independent Spent Fuel Storage Installations stored on Beaver Valley property), they would not see any search results because they do not have read permission for Beaver Valley Independent Spent Fuel Storage Installations; therefore, users may think the documents do not exist in SLES. In essence, if users have not already obtained the need-to-know to read a document, they will not even be able to search for it.

- SLES is slow to upload documents – Security inspectors typically upload into SLES the licensees' security plans and other plant information that are provided by licensees on CDs. Depending on the amount of information provided, uploading the CDs may take several hours, or even days, to complete. Inspectors are required to be present at the workstation during the entire upload process since they are dealing with SGI, and this upload process *must occur* at a shared kiosk workstation because personal SLES desktop terminals do not accept removable media such as CDs.

- Nuclear power plant based resident inspectors' SLES laptops are not set up/functional – Several regional inspectors based in regional offices complained that many resident inspectors either had their SLES laptops stored in a desk and not set up, or they had the laptops set up but not functioning because of expired user certificates due to non-use. Resident inspectors claimed the primary reason for this was because they rarely work with SGI; however, non-functioning SLES laptops can inhibit visiting regional inspectors because the non-functionality precludes easy electronic access to SGI and it encourages the regional inspectors to mail and use paper SGI when conducting power plant inspections.

  Several security inspectors at NRC headquarters told auditors that they would like to have a portable device, such as a tablet, to store and carry SGI with them during their power plant inspections. The tablet would not need to have access to the Internet or any networks, but would be able to hold previously downloaded SGI in electronic format. OIG notes that this may provide more security than hand-carrying SGI and would likely make the inspection process more efficient. An OIS IT specialist reported that there is

currently a tablet pilot underway in NRC's Region II office, but at this time there are no plans to involve SGI in this pilot.

- It can be difficult to read maps and drawings in SLES – Security inspectors will often get electronic maps and drawings from licensees as part of their security documentation. These items are difficult to read at times, due to either being too small to see on the SLES monitor or too large to easily view everything on one page. Therefore, inspectors typically must print these items.

- SLES contains no audio capabilities – There are times when licensees provide security inspectors CDs or DVDs that contain video/audio presentations. While SLES has video capability, it cannot play any sound.

Another goal for the development of SLES was to reduce the amount of SGI paper documents and the overall volume of SGI document storage space. While SLES has reduced a large volume of SGI paper documents, there still remains a large amount within the agency. For example:

- All offices provided NSIR their SGI documents to be input into SLES; however, certain offices continue to maintain paper copies as well. According to an Office of the Secretary staffer, the office is to maintain their SGI documents as official records to meet National Archives and Records Administration requirements. Additionally, an enforcement specialist in one of NRC's regional offices asserted that regulations[17] state that all unclassified SGI paper documents related to enforcement actions that are not considered "significant" must be kept at least 2 years.

- Certain individuals hold on to their SGI documents because there is no formal workflow process whereby users are notified when their documents have been entered into SLES. Due to this uncertainty, some people prefer to maintain a hard copy of documents they submitted.

- NRC regional offices still maintain SGI safes.

[17] NRC Comprehensive Records Disposition Schedule, NUREG-0910, Revision 4.

- NSIR maintains approximately 23 lock bar cabinets containing SGI. In addition, NSIR stores some SGI in General Services Administration-approved safes intended for classified information.

- Within NRC headquarters, an "OIS Vault" contains roughly 375 cubic feet of NRC's confidential documents, including SGI. The vault, a locked room approximately the size of a standard conference room, once served as the official storage area for the agency's sensitive documents prior to the creation of the Agencywide Documents Access and Management System and SLES. It is unknown exactly how many SGI documents are stored in the vault, although OIS management estimates that roughly one-half to three-fourths of the documents within the vault are SGI.

While the agency still maintains a large amount of SGI paper documents, NSIR nonetheless has made progress in reducing the overall volume of SGI paper documents. Since 2010, NSIR has removed over 80 SGI lock bar cabinets from its office space alone. In addition, while the regional offices still maintain some SGI cabinets or safes, regional staff claim the amount of SGI paper documents and SGI lock bar cabinets has been greatly reduced since NSIR began its paper reduction efforts. NSIR is still actively trying to eliminate SGI paper documents and lock bar cabinets and is currently teaming up with OIS to address the OIS vault in the near future.

SLES Is Not a High Priority

SLES has not fully met its users' needs because SLES has not been given a high priority by NRC management. Specifically:

- There is no single individual who serves as a business champion for integrating SLES into the NRC business process.
- The communication channels to discuss system issues between SLES staff and its users are insufficient.

No SLES Business Champion

While OIS and NSIR are both involved with SLES, there is no single individual who serves as a business champion for SLES and its

processes. OIS is responsible for the IT and technical aspects of SLES, but business processes and policy are not under its purview. This responsibility falls under NSIR; however, the individual from NSIR who managed the system prior to its transfer to OIS is no longer employed by NRC. While this former NSIR employee continued to oversee SLES following its transfer to OIS, this was done on a strictly voluntary basis. After SLES was transferred to OIS, NSIR staff claim they provided guidance to OIS but technically no longer had any direct day-to-day SLES responsibilities; the office relies on its contractor to fulfill its records management responsibilities. A separate division within NSIR handles SGI and its policies, but its core duties do not include SLES.

As NSIR and OIS are two distinct entities involved with SLES, there is no clear reporting structure that places someone in charge of – and who understands – both the IT and the business policy side of SLES. As an example, one possible solution identified by OIG to expedite uploads into SLES could be to change some of the existing thin client kiosks to fat clients[18] for users who do a large amount of SGI uploading from CDs. An OIS official stated that this is theoretically possible, but it lacks the independent authority to make this change due to physical security concerns with fat client machines. Such a move would require not only upper management approval, but NSIR's involvement as well.

Another issue is that many people have yet to embrace the use of SLES, and because they are not required to use the system, they continue to work with SGI paper documents. As noted earlier in the report, security inspectors will often mail SGI to power plants prior to their inspections for their use, and individuals and offices are often permitted to maintain their SGI paper documents after the documents have been uploaded into SLES. Additionally, SLES is not used for any formal concurrence process involving SGI; only SGI paper documents are used for this purpose.

[18] All SLES kiosks are composed of thin clients. A thin client is a computer which depends heavily on some other computer (its server) to fulfill its traditional computational roles. Thin clients are barebone computer setups that do not contain any processors or data storage devices – they can be something as minimalistic as a monitor with a keyboard or mouse. A fat client is a networked computer with most resources installed locally, rather than distributed over a network as is the case with a thin client. Some advantages of fat clients are a reduced load on the server and an ability to work independent of the central server. A fat client can also run faster than a thin client since fat clients store many applications locally. However, thin clients are easier to protect from security risks and offer lower maintenance costs.

Communication Is Insufficient

Communication channels to discuss system issues between SLES staff and its users are also inadequate. In the earlier years of SLES while the system was still under NSIR's ownership, NSIR would issue periodic newsletters providing updates about the system. Furthermore, users could join the E-Safe Enhancement Working Group to discuss system issues on a biweekly basis. The newsletters and working groups have since been discontinued and many users are unaware of how to voice their concerns with the system. When OIG relayed the common user complaints to OIS, OIS staff were unaware of some of these system issues. In addition, one of the SLES regular users said the subject matter experts, the individuals who created or owned the SGI, were never consulted as to how the documents should be titled or categorized. This led to extra difficulty in locating files within SLES. When he later tried to approach the SLES team about this matter, he said the team was not receptive to his recommendations or ideas.

OIG notes that information system change control boards are considered a best business practice for ensuring information system stakeholders' concerns are raised and analyzed over a system's lifecycle so that necessary improvements can be made to the system to meet user needs. *National Institute of Standards and Technology Special Publication 800-128* defines a change control board as a group that represents various organization perspectives that has the collective responsibility and authority to review and approve changes to an information system. According to Special Publication 800-128, the board is a check and balance on configuration change activity, assuring that changes are held to organizationally defined criteria (e.g., scope, cost, impact on security) before being implemented.

Though the communication channels between SLES staff and its system users need improvement, it should be noted that the majority of SLES users remarked that they are very pleased with the SLES help desk and the overall support received. An OIS employee also stated that OIS would always try to address any user's concerns as long as OIS is aware of the problem. For example, during the course of this audit, OIG learned that NRC's Technical Training Center did not have access to SLES even though it provides training to security inspectors. OIG notified OIS of the

issue and OIS immediately contacted individuals at the Technical Training Center to discuss the matter. OIS has since approved the change and anticipates installing four SLES workstations at the Technical Training Center by the end of March 2013.

SLES Not Utilized To Its Potential, Possibly Resulting in Fiscal Waste

SLES is not used to its potential and more resources must be used to maintain paper records possibly resulting in fiscal waste. OIS staff reported that SLES has roughly 620 total user accounts, but approximately only 50 "regular"[19] SLES users. Furthermore, according to a Property Management Specialist in the Office of Administration, each lock bar cabinet/safe that stores SGI costs $1,054, and the safes, in particular, are "flying off the shelves." Using SLES on a consistent basis would promote efficiency and would likely reduce paper, printing, mailing, and storage costs.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Designate an SLES business champion from senior management to integrate SLES into NRC business practices.

2. Establish a formal workflow process, similar to that used for the Agencywide Documents Access and Management System, to communicate the status of SLES (E-Safe) file uploads to SGI owners.

3. Evaluate and update the current folder structure to meet user needs.

4. Publish a folder guide to help users identify where SGI is stored within SLES.

5. Develop and implement a retrievable communication plan to communicate SLES updates, changes, etc., and to invite user feedback.

[19] OIS termed a regular user as someone who logged into SLES at least 4 times in the previous 30 days. This does not include administrator accounts used by support personnel.

6. Develop and implement a change control process to routinely evaluate and implement any changes to SLES. Include members from the technical (OIS) and policy (NSIR) sides of SLES, as well as a representative from a Regional office, and gather user concerns from the SLES community.

B. Access Rights Are Inconsistent

Federal regulations mandate security controls to protect systems and networks from inappropriate access and unauthorized use. SLES access rights do not consistently meet the intent of the SGI "need-to-know" requirement or an information system's "least privilege" principle because there is no standard process for granting SGI access to individuals or for verifying user access rights. Providing SLES users access rights that exceed an individual's need-to-know or go beyond organizational business needs increases the risk that SGI could be compromised. Additionally, not having a formal policy in place limits access to some individuals who may need SGI access to effectively do their jobs.

The "Need-To-Know" Requirement and "Least Privilege" Principle

Federal regulations mandate security controls to protect systems and networks from inappropriate access and unauthorized use. Per Title 10, Code of Federal Regulations, Section 73.2 (10 CFR 73.2), *"need-to-know"* means a determination by a person having responsibility for protecting SGI, such as the originator of the material, that a proposed recipient's access to SGI is necessary in the performance of official, contractual, licensee, applicant, or certificate holder employment. Additionally, 10 CFR 73.22 requires that anyone requesting access to SGI must meet this need-to-know requirement. Except as the Commission may otherwise authorize, no person may disclose safeguards information to any other person.

Federal Government internal controls standards for information systems recommend access security controls to protect systems and networks from inappropriate access and unauthorized use. Specifically, the *National Institute of Standards and Technology Guidance Special Publication 800-53* recommends the "least privilege" principle. Simply put, the principle of least privilege requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more.

SLES Folder Access Is Inconsistent With Need-To-Know Requirement and Least Privilege Principle

SLES access rights do not consistently meet the intent of the SGI need-to-know requirement or an information system's least privilege principle. As mentioned in the background section of this report, SLES users gain access to SGI documents by having their branch chief contact the SLES help desk and providing this authorization. However, this does not align with standard SGI policy stated in the Code of Federal Regulations which states that the person responsible for protecting the SGI, such as the document owner, is responsible for providing the need-to-know authorization. An NSIR staff member responsible for standard SGI policy told OIG he was unaware that the SLES policy was different from the regulation until OIG brought it to his attention. He remarked that this discrepancy could be an issue because a branch chief technically does not have the authority to grant need-to-know access since the branch chief is not the originator or possessor of the document. He agreed that the SLES policy is not consistent with the NRC Management Directives or the regulation. In essence, SLES allows users to gain access to SGI without contacting the protector or owner of the information.
The least privilege principle may also be violated if users receive access to folders and documents simply by belonging to a user group. As mentioned in the background section of the report, SLES stores all SGI documents in folders with other related SGI documents. To receive access to a particular folder, users must be part of a user group with read permission to that folder. However, user groups may also have access to several different folders within SLES.

Therefore, when users need access to a given document, they receive access to all documents within that particular folder as well as to several other folders they may not need. Essentially, users receive access to SGI documents based on the user groups they belong to and not based on the principle of accessing only the information they need to perform their jobs.

While several SLES users may have access to documents they may not need, a common complaint by users – especially by those in the regions – is that they do not readily have access to documents they do need in SLES, and that the branch chief approval process is inefficient. One resident inspector claimed that he could not access any SLES documents related to his own power plant without first getting approval from his offsite

branch chief. Until this is changed, he said he would not use SLES because it is a major inconvenience. He stated that he has to "jump through hoops" to get the necessary approval to access his own plant's documents and that it was simply easier to go to the licensee's safe and view SGI documents there.

Several users commented that getting the approval to access SLES documents is sometimes untimely and burdensome depending on the availability of the branch chief or how long it may take the branch chief to contact the SLES help desk. Since the process is not always efficient, some users claim they simply go directly to the licensee or contact someone in NSIR to obtain access to documents in SLES.

There Is No Standard Process for Granting or Verifying Access to SGI

SLES access rights do not consistently meet the intent of the SGI need-to-know requirement or an information system's least privilege principle because there is no standard process for granting SGI access to individuals or for verifying user access rights. Since there are no owners of SGI folders or documents within SLES,[20] user access is provided rather haphazardly by the SLES help desk. The complicated system setup of assigning individuals to user groups with specific permissions to folders containing SGI does not allow for the need-to-know requirement and least privilege principle to be easily followed. While the SLES help desk provides access to SGI, it is only doing as instructed by the individual branch chief (who is simply acting on behalf of each requesting user). And although the help desk and SLES program in general are run by OIS, OIS is not familiar with – or responsible for – the SGI need-to-know policies; this responsibility belongs to NSIR.

NRC also lacks procedures to conduct a periodic review of user folder access. After reviewing SLES user records, OIG interviewed 27 NRC employees who had read rights to folders within SLES. Of the 27 interviewed, 4 claimed that they had read rights to more folders than they needed and 18 stated they did not need access to SLES at all.

[20] Due to the sensitive nature of the information, there are only two SLES folders that have an actual folder owner: Target Sets and Force on Force, which are overseen by an individual in NSIR. Only the assigned folder owner can make the need-to-know determination when users request access.

Furthermore, eight SLES user accounts belonged to people no longer employed by NRC.[21] In sum, there was no process to identify users who no longer needed access to SLES or who may have only required limited access.

SGI Could Be Compromised

Granting SLES users access rights that exceed individual or organizational business needs increases the risk that SGI could be intentionally or accidentally compromised. Tighter enforcement of the need-to-know requirement and least privilege principle to NRC staff that use SLES would provide an automated control to prevent possible data loss. On the other hand, rules should not be so strict that they limit NRC staff from effectively conducting their jobs. By having a formal policy in place that takes into account the user's needs and responsibilities, NRC staff may be able to use SLES more effectively while limiting security risks.

Recommendation

OIG recommends that the Executive Director for Operations:

7. Develop a structured access process that is consistent with the SGI need-to-know requirement and least privilege principle. This should include:

- Establishing folder owners within SLES and providing the owners the authority to approve the need-to-know authorization (as opposed to branch chiefs).
- Conducting periodic reviews of user access to folders.
- Developing a standard process to grant user access.

[21] In the cases of ex-NRC staff still having SLES accounts, the risk is mitigated because a Personal Identity Verification card is required to log into SLES. Employee exit procedures are in place to ensure that employees surrender their Personal Identity Verification cards at the conclusion of their NRC employment.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Designate an SLES business champion from senior management to integrate SLES into NRC business practices.

2. Establish a formal workflow process, similar to that used for the Agencywide Documents Access and Management System, to communicate the status of SLES (E-Safe) file uploads to SGI owners.

3. Evaluate and update the current folder structure to meet user needs.

4. Publish a folder guide to help users identify where SGI is stored within SLES.

5. Develop and implement a retrievable communication plan to communicate SLES updates, changes, etc., and to invite user feedback.

6. Develop and implement a change control process to routinely evaluate and implement any changes to SLES. Include members from the technical (OIS) and policy (NSIR) sides of SLES, as well as a representative from a Regional office, and gather user concerns from the SLES community.

7. Develop a structured access process that is consistent with the SGI need-to-know requirement and least privilege principle. This should include:
    - Establishing folder owners within SLES and providing the owners the authority to approve the need-to-know authorization (as opposed to branch chiefs)
    - Conducting periodic reviews of user access to folders.
    - Developing a standard process to grant user access.

V. AGENCY COMMENTS

At an exit conference on March 20, 2013, agency management stated their agreement with the findings and recommendations in this report. Agency management also provided supplemental information that has been incorporated into this report, as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

Appendix

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The audit objective was to determine if SLES meets its operational capabilities and applicable security controls.

SCOPE

The audit focused on reviewing the SLES system and ensuring it meets user needs while complying with security requirements. We conducted this system audit at NRC headquarters from July 2012 through December 2012. 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, or misuse in the program.

METHODOLOGY

OIG reviewed relevant Federal regulations and internal/external guidance including:

- Code of Federal Regulations, Title 10, Part 73, Section 22, "Protection of Safeguards Information: Specific Requirements."
- The Paperwork Reduction Act of 1995.
- National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations."
- A Staff Requirements Memorandum M040114A, "Briefing on the Status of OCIO Programs, Performance, and Plans."
- Management Directive 12.7, "NRC Safeguards Information Security Program."
- National Institute of Standards and Technology Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems."
- OIG-12-A-12, "Audit of NRC's Protection of Safeguards Information."

Auditors also used the SLES system and reviewed hundreds of SLES folders, user groups, user names, and permissions in conducting data analysis and identifying any possible trends.

At NRC headquarters, in Rockville, Maryland, auditors interviewed NSIR and OIS staff, including contractors assigned to both NSIR and OIS, to gain an understanding of their roles and responsibilities related to the SLES system. Auditors also conducted numerous telephone interviews of NRC regional staff, resident inspectors, and NRC headquarters staff and management who were listed as SLES users. Auditors viewed a demonstration of the SLES system and also witnessed a failover test conducted by NSIR illustrating the redundant features of SLES.

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 work was conducted by Beth Serepca, Team Leader; Rebecca Underhill, Audit Manager; Larry Vaught, Senior Auditor; and Michael Blair, Senior Management Analyst.