AUDIT REPORT

Audit of NRC's Protection of Safeguards Information

OIG-12-A-12 April 16, 2012

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 16, 2012

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S PROTECTION OF SAFEGUARDS INFORMATION (OIG-12-A-12)

Attached is the Office of the Inspector General's (OIG) audit report titled, *Audit of NRC's Protection of Safeguards Information.*

The report presents the results of the subject audit. Agency comments provided at the March 28, 2012, 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 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, Team Leader, Security and Information Management Audit Team, at 415-5911.

Attachment: As stated

EXECUTIVE SUMMARY

BACKGROUND

Safeguards Information, or SGI, is a category of sensitive unclassified information that is unique to the Nuclear Regulatory Commission (NRC). SGI is detailed security-related information that identifies security measures for the physical protection of special nuclear material, or security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. Unauthorized disclosure of SGI could have a significant adverse effect on public health and safety and/or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of materials or facilities subject to NRC jurisdiction. Such an unauthorized release could result in damage to the Nation's critical infrastructure, which includes nuclear power plants and certain other facilities and radioactive materials licensed and regulated by the NRC.

Access to SGI is restricted to personnel who have an established ''need-to-know'' the information and are also deemed "trustworthy and reliable" by undergoing a background check and a Federal Bureau of Investigation criminal history records check. A security clearance is not needed to access SGI. While most people who consistently deal with SGI are NRC employees or licensees, access to SGI is not contingent upon one's relationship with NRC. For example, contractors, consultants, private citizens who participate in adjudicatory hearings, and qualified private citizens who choose to comment on certain regulatory guides can gain access to SGI if they meet the regulatory requirements stated above.

Hardcopy and electronic documents containing SGI must be protected in accordance with NRC regulations and guidance. When in use, documents containing SGI must always be under the direct control of the authorized user of the information. These documents must be protected to avoid disclosing the information to unauthorized persons. Within NRC, this means that hardcopy SGI documents are stored in locked security containers, while electronic copies are stored in the Safeguards Local Area Network and Electronic Safe (SLES). SLES is NRC's electronic document management system for the storage of electronic SGI documents.

NRC has given a select group of individuals within the agency the authority to review security documents to determine whether the items contain SGI and therefore warrant protection. These individuals are referred to as SGI designators, and the majority of offices have at least one designator. The SGI designator role is a collateral duty and employees must fulfill training requirements to become certified to perform the role. Only individuals who have been certified as SGI designators can make SGI determinations.

OBJECTIVE

The audit objective was to determine if NRC adequately ensures the protection of SGI.

This audit was conducted to follow up on an audit issued in January 2004, OIG-04-A-04*, Audit of NRC's Protection of Safeguards Information*. The 2004 audit found that the benefit of having an SGI program was unclear and that NRC lacked a central authority for controlling, coordinating, and communicating SGI program requirements. The audit also found examples in which NRC and licensee representatives inappropriately released SGI to unauthorized individuals.

RESULTS IN BRIEF

Since the 2004 audit, NRC has made improvements to the SGI program, including the development of a Management Directive specifically for SGI and identification of a lead program office for developing SGI policies and procedures. However, the Office of the Inspector General identified the following areas for further improvement of the SGI program: NRC (1) lacks a structured process for tracking SGI releases, (2) lacks guidance on granting "outsiders" access to SGI, and (3) has inadequate business processes over the SGI designator role.

RECOMMENDATIONS

This report makes recommendations to improve the agency's SGI program. A list of these recommendations appears on page 20 of this report.

AGENCY COMMENTS

At an exit conference on March 28, 2012, agency management stated their general 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

ADM	Office of Administration
CFR	Code of Federal Regulations
CSO	Computer Security Office
DFS	Division of Facilities and Security
DSO	Division of Security Operations
IT	Information Technology
MD	Management Directive
NRC	U.S. Nuclear Regulatory Commission
NSIR	Office of Nuclear Security and Incident Response
OEDO	Office of the Executive Director for Operations
OIG	Office of the Inspector General
OIS	Office of Information Services
SGI	Safeguards Information
SLES	Safeguards Local Area Network and Electronic Safe

TABLE OF CONTENTS

APPENDIX

I. BACKGROUND

Safeguards Information, or SGI, is a category of sensitive unclassified information[1] that is unique to the Nuclear Regulatory Commission (NRC). SGI is detailed security-related information that identifies security measures for the physical protection of special nuclear material,[2] or security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. Unauthorized disclosure of SGI could have a significant adverse effect on public health and safety and/or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of materials or facilities subject to NRC jurisdiction. Such an unauthorized release could result in damage to the Nation's critical infrastructure, which includes nuclear power plants and certain other facilities and radioactive materials licensed and regulated by the NRC.

Access to SGI is restricted to personnel who have an established ''need-to-know''[3] the information and are also deemed "trustworthy and reliable"[4] by undergoing a background check and a Federal Bureau of Investigation criminal history records check.[5] Additionally, a security clearance is not needed to access SGI. While most people who consistently deal with SGI are NRC employees or licensees, access to SGI is not contingent upon one's relationship with NRC. For example, contractors, consultants, private citizens that participate in adjudicatory hearings, and qualified private citizens that choose to comment on certain regulatory guides can gain access to SGI if they meet the regulatory requirements stated above.

[1] Other categories of sensitive unclassified information include proprietary information, allegation information, and personally identifiable information.
[2] "Special nuclear material" is defined by the Atomic Energy Act of 1954, as amended, as plutonium, uranium-233, or uranium enriched in the isotopes uranium-233 or uranium-235.
[3] 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 that a proposed recipient's access to SGI is necessary in the performance of official, contractual, licensee, applicant, or certificate holder employment.
[4] Per 10 CFR 73.2, *trustworthiness and reliability* are characteristics of an individual considered dependable in judgment, character, and performance, such that disclosure of SGI to that individual does not constitute an unreasonable risk to the public health and safety or common defense and security. A determination of trustworthiness and reliability for this purpose is based upon a background check.
[5] Per 10 CFR 73.59, certain individuals do not need background checks prior to receiving access to SGI, such as (a) an employee of the Commission or the Executive Branch of the U.S. Government who has undergone fingerprinting for a prior U.S. Government criminal history records check; (b) a member of Congress; (c) the Governor of a State or his or her designated State employee representative; and (d) Federal, State, or local law enforcement personnel, among others.

Hardcopy and electronic documents containing SGI must be protected in accordance with NRC regulations and guidance.[6] When in use, documents containing SGI must always be under the direct control of the authorized user of the information. These documents must be protected to avoid disclosing the information to unauthorized persons. Within NRC, this means that hardcopy SGI documents are stored in locked security containers, while electronic copies are stored in the Safeguards Local Area Network and Electronic Safe (SLES). SLES is NRC's electronic document management system for the storage of electronic SGI documents.

NRC has given a select group of individuals within the agency the authority to review security documents to determine whether the items contain SGI and therefore warrant protection. These individuals are referred to as SGI designators, and the majority of offices have at least one designator. The SGI designator role is a collateral duty and employees must fulfill training requirements to become certified to perform the role.

Only individuals who have been certified as SGI designators can make SGI determinations. Management Directive (MD) 12.7 outlines the requirements that an individual must follow to be granted this certification. Specifically, there is a series of training modules that the individual must complete that covers specific SGI designator training. Once this training is completed, the employee sends his/her training certificates to the Office of Nuclear Security and Incident Response (NSIR) for review. An NSIR official places the individual on the certified designator list.

In addition to paper documents, individuals work with electronic SGI within SLES. To gain SLES access, a user must complete an application form and submit it to the Office of Information Services (OIS). There are two levels of access that a user can obtain: viewer and designator. The viewer role allows users only to view documents that they have been granted permission to see. The designator role has the same features as the viewer role, but also allows the user to generate SGI documents within the system. To be granted the SLES designator access level, the user

[6] All media containing SGI, such as laptop computers or removable magnetic media (e.g., hard drives or compact disks), fall under the same regulations and guidance as hardcopy and electronic documents and must be protected accordingly.

must be a certified SGI designator and must submit the required training documentation to OIS.

Regulations and Orders

The Atomic Energy Act of 1954, as amended, provides NRC the authority to prescribe regulations to protect SGI. This Federal law also states the requirements for the criminal history records check in order to access SGI. The Code of Federal Regulations (Title 10, Part 73) establishes the general licensee performance requirements to protect SGI.

NRC has seven management directives that provide guidance to staff concerning the protection of information, including SGI:

1. MD 12.7 – *NRC Safeguards Information Security Program*, provides information security policy associated with the preparation, handling, distribution, accountability, and protection of SGI.
2. MD 12.6 – *NRC Sensitive Unclassified Information Security Program*, provides measures to ensure that sensitive unclassified information is handled appropriately and is protected from unauthorized disclosure.
3. MD 12.5 – *NRC Automated Information Security Program*, provides security measures to protect NRC information and information systems, including any hardware or software that is used to process, store, or transmit SGI.
4. MD 12.2 – *NRC Classified Information Security Program*, provides the proper procedures for all NRC personnel responsible for handling classified information.[7]
5. MD 12.1 – *NRC Facility Security Program*, provides measures to ensure that SGI and classified information is protected from unauthorized disclosure and that assets in NRC facilities are protected from harm, loss, or misuse.
6. MD 7.4 – *Reporting Suspected Wrongdoing and Processing OIG Referrals*, provides direction and guidance for reporting suspected wrongdoing to the Office of the Inspector General (OIG).
7. MD 3.4 – *Release of Information to the Public*, provides NRC staff general policy guidance on the release of agency information to the public.

[7] While MD 12.2 focuses on classified information, there is a correlation with SGI as the SGI program is modeled after the classified program according to NRC management.

Offices Involved

The primary NRC offices involved with the SGI program are NSIR, OIS, the Office of Administration (ADM), and the Computer Security Office (CSO).

NSIR's Division of Security Operations (DSO) is the SGI program owner and is responsible for developing and overseeing the implementation of NRC requirements and activities related to safeguards and security for NRC licensed facilities and activities. DSO is responsible for ensuring the protection of SGI and classified information at NRC facilities and by NRC contractors and licensees by planning, coordinating, and managing the information security program. DSO runs the SGI training program for NRC employees and administers NRC's SGI designator program.

OIS is responsible for providing expertise on NRC's information technology (IT) infrastructure, including security monitoring, assessment, incident response, and integration of automated solutions to proactively mitigate IT security vulnerabilities. OIS plans, develops, and delivers programs and services related to the storage, retrieval, protection, and preservation of NRC information in paper and electronic media. Regarding SGI, OIS owns and supports the infrastructure that SLES runs on and is responsible for granting appropriate user access.

Within ADM, the Division of Facilities and Security (DFS) establishes policy and plans and directs the agency's building management and facilities and personnel security programs. DFS administers the NRC security program for physical security and is responsible for physically protecting NRC facilities, ensuring the safeguarding of classified and sensitive unclassified information at NRC and NRC contractor facilities, and coordinating with other law enforcement agencies on related matters.

CSO, specifically the Cyber Situational Awareness, Analysis, and Response Team, is in charge of tracking, monitoring, and reporting NRC computer security incidents. CSO monitors NRC's IT security vulnerabilities, maintaining an awareness of the threat to NRC's IT infrastructure. This office conducts trend analysis of events and recommends actions to minimize or prevent releases of information. CSO handles electronic releases and NRC internal SGI policy that involves IT systems.

Unauthorized Releases of SGI

An SGI "release" is any situation where SGI information has been inadequately protected.[8] In the worst case scenario, a release results in an unauthorized individual seeing the sensitive information. However, there are many instances when that release does not result in any unauthorized access. For example, a document owner may leave SGI on his/her desk before realizing it later, or an NRC employee may not take the proper security steps when emailing an SGI document to another authorized user. Based on the scenario and type of release, the MDs require that all NRC employees report SGI releases to specific NRC offices. While the specific reporting offices are mentioned in the MDs, there are no clearly quantifiable timeliness requirements for reporting SGI releases.

II. OBJECTIVE

The audit objective was to determine if NRC adequately ensures the protection of SGI. The report appendix provides information on the audit scope and methodology.

This audit was conducted to follow up on an audit issued in January 2004, OIG-04-A-04*, Audit of NRC's Protection of Safeguards Information*. The 2004 audit found that the benefit of having an SGI program was unclear and that NRC lacked a central authority for controlling, coordinating, and communicating SGI program requirements. The audit also found examples in which NRC and licensee representatives inappropriately released SGI to unauthorized individuals.

[8] Any "release" that is reported to DFS is also called an infraction as part of NRC's Security Infraction Program. A security infraction is a failure to comply with NRC security requirements or procedures. This infraction category includes many types of issues, including actual or suspected compromises of SGI, failure to properly escort uncleared visitors, or loss of a badge under circumstances of negligence.

III. FINDINGS

Since the 2004 audit, NRC has made improvements to the SGI program, including the development of a management directive specifically for SGI and identification of a lead program office for developing SGI policies and procedures. However, OIG identified the following areas for further improvement of the SGI program: NRC (1) lacks a structured process for tracking SGI releases, (2) lacks guidance on granting "outsiders" access to SGI, and (3) has inadequate business processes over the SGI designator role.

A. Lack of a Structured Process for Tracking SGI Releases

While SGI releases are reported to NRC offices identified to record and respond to such incidents, the total universe of SGI releases is not known to NRC management. The universe of SGI releases is unknown because NRC does not have a structured, streamlined process for reporting and tracking releases. Without a full understanding of the universe of releases, NRC cannot trend releases to see if there is a systemic problem that could be resolved from additional guidance, or if clarifications to existing guidance need to be made.

Reporting Requirements

NRC managers involved with the SGI program should have access to complete information about SGI releases in a timely manner to respond to problems and improve the overall SGI program. NRC MDs provide guidance to employees on how to report problems concerning SGI. MD 12.7 is the overarching guidance document for SGI; however, several other MDs address the handling of various SGI releases. For example, MD 12.5 discusses computer-related issues with SGI, while MD 3.4 discusses all releases of information to the public.

Universe of SGI Releases Is Unknown

While SGI releases are reported to NRC offices assigned to record and respond to such incidents, the total universe of SGI releases is not known to NRC management. Based on the guidance provided in the MDs, employees report their SGI releases to one or more of the following five NRC offices: CSO, NSIR/DSO, ADM/DFS, Office of the Executive Director for Operations (OEDO), and OIG. Four of these offices maintain their own file system to keep track of the releases reported. For example, ADM/DFS maintains a spreadsheet that has the date the release occurred, the date it was reported, the offices and individuals involved, and a description of the release, while OEDO maintains a file folder containing the notifications the office has received. CSO and OIG also maintain some records; however, NSIR/DSO does not maintain any files for tracking SGI releases.

OIG performed an analysis to identify the total universe of SGI releases that were reported to CSO, ADM/DFS, OEDO, and OIG between March 11, 2005, and October 4, 2011.[9] During this timeframe, a total of 95 unique releases were reported to and recorded by the respective offices. Of these 95 releases reported, 91 were reported to only one office (see Table 1). Additionally, OIG identified four releases that were simultaneously reported to two offices (see Table 2). There were no releases reported to more than two offices. Tables 1 and 2 below show a breakdown of the number of reported cases and to which office they were reported.

Table 1. Single Reported Releases

Source	Total	2005	2006	2007	2008	2009	2010	2011
CSO	31		6	7	5	5	2	6
ADM/DFS	51				15	15	11	10
OEDO	5	3					1	1
OIG	4		1	1	2			
Issues Reported to One Office	91	3	7	8	22	20	14	17

Table 2. Dual Reported Releases

Source	01/03/2008	10/19/2010	02/02/2011	09/27/2011
CSO	1			1
ADM/DFS	1	1	1	
OEDO		1		1
OIG			1	
Issues Reported to Two Offices	1	1	1	1

OIG also analyzed the length of time taken for releases to be reported. Of the 95 infractions reported between March 11, 2005, and October 4, 2011, 56 (59 percent) were reported on the same day that the release occurred, 15 (16 percent) were reported between 1 and 5 days, 14 (15 percent)

[9] The purpose of OIG's analysis was to identify the universe of reported releases and not to assess whether releases were reported to the proper entity.

were reported between 6 and 30 days, 2 (2 percent) were reported between 31 and 60 days, 4 (4 percent) were reported between 61 and 100 days, and 4 (4 percent) took longer than 100 days to report. The following chart provides a breakdown of the timeliness of the releases reported:

Table 3. Release Report Days

Days Between SGI Release and Reporting	# of Infractions Reported	Percentage of Releases Reported In Each Time Period
0	56	59%
1 – 5	15	16%
6 – 30	14	15%
31 – 60	2	2%
61 – 100	4	4%
>100	4	4%
Totals	95	100%

* Percentage rounded to whole percentage point

Lack of a Structured Process for Reporting

NRC management does not know the universe of SGI releases because the agency lacks a structured, streamlined process for reporting and tracking releases. NRC has several MDs that explain and outline how various releases should be reported, but these directives contain different reporting requirements and there is no requirement for any single entity to keep track of all the reporting that occurs. MD 3.4, *Release of Information to the Public*, states that the OEDO and OIG should be notified of any release, in writing. Additionally, it states that NSIR must be contacted, but it does not state if this notification needs to be in writing. It further states the CSO should be contacted if the release involved IT systems. MD 7.4, *Reporting Suspected Wrongdoing and Processing OIG Referrals*, states that OIG should be notified if there is a willful violation with SGI. MD 12.1, *NRC Facility Security Program*, states that DFS should be notified, in writing, of any infractions and violations. MD 12.5, *NRC Automated Information Security Program*, states that CSO should be notified with any release related to computers.[10] MD 12.7, *NRC Safeguards Information*

[10] MD 12.5 identifies NRC's Office of the Chief Information Officer as having the responsibility to respond to incidents involving NRC systems that are processing sensitive information, SGI, and classified information. However, in October 2007, CSO was created and the Cyber Situational Awareness, Analysis, and Response Team was tasked with the responsibilities outlined in MD 12.5 for responding to computer security incidents, including SGI releases.

Security Program, states that DFS, NSIR/DSO, OEDO, and OIG should be notified of any release involving SGI. While MD 12.2, *NRC Classified Information Security Program*, provides guidance for the protection of classified information, it does not provide any information on how to report releases related to SGI.

To add to the confusion, MD 12.7 incorrectly restates the reporting requirements listed in MD 3.4 when dealing with SGI releases to the public. MD 12.7 states that when reporting any inadvertent SGI release, DFS, DSO, OEDO, and OIG should be contacted. However, in MD 3.4, DFS is not listed as an office that should be contacted. The following chart is a breakdown of the MDs and the offices that are required to be notified for the various types of SGI releases:

Table 4. MD Reporting Requirements

MD	Office				
	ADM/DFS	NSIR/DSO	OEDO	OIG	CSO
3.4		x*	x	x	x
7.4				x	
12.1	x				
12.5					x
12.7	x	x	x	x	

* Note: MD 3.4 states that NSIR must be notified but does not specify which office within NSIR (e.g., DSO) should be contacted.

While a DSO official stated that they have tried to model the SGI program after the classified information program, this is not the case when it comes to reporting SGI releases. According to MD 12.2, *NRC Classified Information Security Program*, there is a single point of contact responsible for receiving all releases related to classified information. However, within the SGI program there is no single point of contact responsible for intake of all of SGI releases. For example, in some cases, NRC senior managers will report the SGI releases to other senior managers in the responsible program offices, but this information is not necessarily reported in a timely manner to the staff responsible for tracking releases. Nevertheless, OIG observed that CSO employs a "best practice" for managing the intake of SGI releases. CSO maintains a tracking system with unique identifier numbers for each release and assigns two points of contact who rotate coverage to ensure someone is always available to receive the reported releases.

Another problem was NRC's mandatory annual online information security training. While this training program conveys to employees what to do if they come across unprotected classified information, it does not provide any information on who to contact or what to do if there is an SGI release.

Compounding the non-streamlined approach to reporting and tracking SGI issues is a lack of communication among the offices involved with SGI. For example, while NSIR is responsible for developing policies related to SGI and DFS is responsible for enforcing these policies, the two offices do not share details on the releases identified. Furthermore, none of the offices that track SGI issues perform trending on the information or provide statistics to other involved offices unless another office requests this information. OIG also identified several instances where the offices involved with SGI did not know who to contact in the other offices to share or obtain information.

No Trending To Facilitate Improvements in SGI Program

Without a full understanding of the universe of releases, NRC cannot trend releases to see if there is a systemic problem that could be resolved from additional guidance, or if clarifications to existing guidance are needed. Furthermore, if trending on SGI releases were performed, NSIR could make changes to the annual training to ensure that sufficient guidance is provided on SGI problem areas.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Develop a structured reporting process that includes:
   - One point of contact to receive reports of all SGI releases.
   - A numbering system to track the number of releases reported in a consistent manner.
   - A system to report information on releases from the central point of contact to the responsible program offices.
     A system to trend releases and to make any needed programmatic changes.

2. Update the affected MDs (3.4, 7.4, 12.1, 12.5, and 12.7) to provide consistent guidance on the new reporting structure outlined in recommendation 1.

3. Develop and implement interim guidance to communicate the structured reporting process to NRC staff.

4. Update the annual online security information training to reflect the reporting requirements for SGI releases.

B. No Guidance for Granting "Outsiders" Access to SGI

While MD 12.7 provides details on many aspects of protecting SGI, it lacks guidance on how to grant SGI access to a non-NRC, non-licensee entity. MD 12.7 lacks information about approving SGI access to outsiders because NSIR, which is responsible for the content of MD 12.7, believes that the existing guidance is sufficient. Without comprehensive guidance, there is no assurance that consistent measures are being taken to protect SGI.

SGI Policy and Guidance

It is NRC's policy to ensure that SGI is properly handled and protected from unauthorized disclosure under pertinent laws, regulations, management directives, and applicable directives of other Federal agencies and organizations. Specifically, MD 12.7, *NRC Safeguards Information Security Program*, provides NRC staff the security requirements for the preparation, handling, distribution, accountability, and protection of SGI. Regarding SGI access, MD 12.7 explains the eligibility requirements to receive SGI, as well as those who are exempt from the specific requirements. According to MD 12.7, NRC employees, consultants, and contractors are all responsible for ensuring that the procedures specified in the document are followed to protect SGI.

In accordance with the regulations, MD 12.7 states that to access SGI, an individual must have a need-to-know the information and is subject to a fingerprinting and FBI criminal history records check. The responsibility of assessing the need-to-know of an individual falls on the owner of the requested SGI document (e.g., the NRC employee who created the document or the individual in possession of the document) per the regulation, 10 CFR Part 73.

Office of Management and Budget Bulletin, M-07-07, "Final Bulletin for Agency Good Guidance Practices," issued in January 2007, provides guidance on the development of policies and procedures within Government agencies. The bulletin explains that well-designed guidance documents serve many important or even critical functions in regulatory programs. Agencies can provide helpful guidance to interpret existing law through an interpretive rule or to clarify how they tentatively will treat or enforce a governing legal norm through a policy statement.

Lack of Guidance on Granting Access to "Others"

While MD 12.7 provides details on various aspects of protecting SGI, it does not communicate a methodology for document owners to use when making determinations to grant non-NRC, non-licensees access to SGI. These individuals, or "outsiders,"[11] may be interveners, vendors, external stakeholders, or members of the general public.

As an example of the need for better guidance in this area, in May 2011, an outsider sought to provide comments on a proposed NRC technical document and asked for permission to view some SGI material that provided support to NRC's technical basis. The document owner, an NRC employee with an extensive security background, was unaware of the proper steps or procedures to grant this access. The NRC employee could not locate any NRC guidance that detailed the steps of providing SGI access to outsiders. Consequently, the employee contacted Office of the General Counsel and NSIR management to develop a plan that would potentially allow the outsider to access SGI.

The NRC employee took additional steps to add a layer of security by asking the outsider to sign a confidentiality agreement, and required the outsider to view the SGI at NRC headquarters only. The steps taken were not listed in any NRC guidance documentation. Accordingly, the document owner expressed frustration because the lack of guidance made the employee feel "on her own" in dealing with this type of situation.

Developing Guidance Not Identified as a Need

MD 12.7 lacks information about approving SGI access to outsiders because NSIR, the owner of MD 12.7, believes that the existing guidance is sufficient. NSIR staff stated that everyone who accesses SGI is subject to the regulation; however, the regulation, like MD 12.7, does not describe a process for granting SGI to outsiders. Rather, regarding SGI access, only the owner responsibility requirement of determining the need-to-know was addressed. Furthermore, when NSIR staff were asked to describe the steps of granting SGI access to outsiders, they could not do so except to say that the regulation must be followed. NSIR confirmed that there were no additional requirements or a separate policy for granting outsiders SGI access, but claimed it was not a necessity as the regulations were

[11] The term "outsiders" is not an industry term and is being used strictly for the purpose of this audit.

clear enough, and NRC staff could obtain assistance directly from NSIR if needed.

One NSIR staff member claimed a confidentiality agreement must be signed when granting outsiders SGI access. However, there are no statutory or regulatory requirements that state the need to use a confidentiality agreement.

No Assurance that Consistent Measures Are Applied To Protect SGI

Without comprehensive guidance, there is no assurance that measures are consistently being applied to protect SGI. There are no clear instructions on how to grant SGI access to outsiders. If the discretion is left solely to each individual document owner, there could be a disparity on the controls used to protect SGI. Document owners may have varying levels of security knowledge and could take different approaches in determining what is sufficient to distribute SGI. This potentially could lead to a security compromise as SGI could be viewed by an ineligible individual or simply handled improperly by an approved outsider.

While the particular example described above did not present any additional known problems, this can be largely attributed to the document owner's extensive security experience and self-admitted propensity for being extremely conscientious. However, this type of situation could very well pose problems for other NRC staff in the future.

Recommendations

OIG recommends that the Executive Director for Operations:

5. Update MD 12.7 to include detailed guidance on granting "outsiders" access to SGI.

6. Develop and issue interim guidance covering how to grant "outsiders" access to SGI.

C. Inadequate Business Processes Over the SGI Designator Role

NRC does not have accurate and complete records on the universe of SGI designators because NRC lacks adequate business processes over the SLES SGI designator role and certified SGI designator list. A lack of accurate SGI designator lists could prevent NRC from communicating policy or procedural changes to those who have this responsibility and ensuring there is adequate SGI designator coverage throughout the program offices.

Structured and Efficient Programs

According to Federal Government guidance, including the Government Accountability Office's "Standards for Internal Control in the Federal Government," a program's efficiency is dependent on (1) clearly delineated roles and responsibilities of offices and individuals involved to avoid confusion and ensure that people understand their roles and responsibilities, (2) guidance documents to establish management expectations and ensure that all staff involved understand their roles, (3) training to ensure that employees have the skills needed to perform their work, and (4) data that is organized to facilitate use by staff and managers for decisionmaking.

Designator Lists Are Inadequate

NRC does not have accurate and complete records on the universe of SGI designators. OIG interviewed 46 NRC employees who were listed on the certified SGI designator list. Of the 46 interviewed, 16 (35 percent) did not know they were on the SGI designator list. Furthermore, 21 individuals (46 percent) have never designated SGI. Several employees had moved offices, changed job functions, or no longer needed to maintain their status as a SGI designator.

One designator said it was embarrassing that she had no idea she had been on the SGI designator list for the past 3 years. She said she was only with NRC for 6 weeks before apparently taking the online SGI designator training course, and was incredulous that she could be considered an SGI designator. Another individual said she had no idea how she became an SGI designator. This individual took several NRC online training classes when she was hired at NRC and assumes that the

SGI designator training course was one of these classes. However, she stated that while she is an NRC employee, she currently does not work in any NRC offices as she is a full-time student. Another employee said there should be some type of yearly designator list scrub, or ongoing competency test, as there was no way he could designate SGI even though he was on the SGI designator list.

After OIG began contacting certified designators, some of these individuals began contacting DSO to be removed from the SGI designator list. At this point, NSIR became aware of a misalignment between the certified designator list maintained by NSIR and the SLES designator role list maintained by OIS. NSIR performed a review of all individuals with SLES designator access and discovered there were 137 SLES designators who were not on the certified SGI designator list. At the request of NSIR, OIS then reviewed each of these 137 individuals to determine if they had the proper training documentation to merit their SLES designator status. Upon completion of the review, OIS was able to provide the proper training documentation for only 17 of the 137 individuals who had the SLES designator status. As a result, OIS changed the SLES status from "designator" to "reader" for the 120 users who lacked sufficient paperwork, and informed the individuals that to regain SLES designator status, they would have to provide sufficient documentation supporting that the prerequisite SGI training requirements had been met.

Lack of a Business Process Over the SGI Designator Role

SGI designator lists are inaccurate because NRC lacks adequate business processes over the SGI designator role. Specifically, there is no coordination or communication between OIS and NSIR, and there are no formal procedures in place to ensure only proper individuals are considered SGI designators.

NSIR and OIS lack coordination and communication regarding the SGI designator role. In granting individuals SLES designator access, OIS has not communicated with NSIR to verify that these individuals are on the certified designator list. There is also no cross-office communication between NSIR and OIS to ensure that the two designator lists match. Furthermore, OIG found that NSIR lacked a specific point of contact within OIS with regard to SLES.

There is also a lack of formal procedures related to the SGI designator role. While there is a clear procedure in place to grant the SGI designator role, there is no process to ensure that the list is properly maintained. The NSIR group responsible for maintaining the certified designator list takes an informal approach to collecting information about individuals who no longer need to be on the list. For example, NSIR staff relies upon their own familiarity with SGI designators, reading the retirement announcements posted on NRC's Web site, and periodically checking the staff directory to determine if the listed designators are still NRC employees.

Furthermore, there is no established procedure to contact employees to determine if they need to maintain their role as a certified SGI designator. OIS does not have any formal procedures to remove SGI designator access from individuals or determine if the users still need to maintain this level of access to the SLES system. Additionally, once an SGI designator is certified, there is no required refresher training to ensure that designators maintain familiarity with their roles and responsibilities.

There are no formal business processes regarding the SGI designator role because management was not aware of this issue. However, since OIG conveyed these issues to NRC during the course of this audit, NSIR and OIS have begun to work together to resolve the issues. In December 2011, OIS and NSIR held a meeting to discuss possible solutions and better controls over the SGI designator role. One resolution from the meeting was to implement a policy that prior to granting any SLES designator access, OIS will first contact NSIR to ensure this individual is a certified SGI designator.

A lack of accurate SGI designator lists could prevent NRC from communicating policy or procedural changes to those who have the SGI designator responsibility, as well as ensuring there is adequate SGI designator coverage throughout the program offices. Furthermore, by requiring periodic refresher training, individuals who want to remain designators would proactively maintain their certifications and familiarize themselves with the SGI policies. Those who are no longer interested in being designators could communicate this by not renewing their certification.

Recommendations

OIG recommends that the Executive Director for Operations:

7. Develop and implement formal business processes for certified SGI designators and the SLES designator role. These procedures should include periodically verifying:
    - The need for individuals to maintain designator role.
    - A match between the certified designator list and the SLES designator user list.

8. Develop and require annual refresher training for the SGI Designator role.

IV. Consolidated List of Recommendations

OIG recommends that the Executive Director for Operations:

1. Develop a structured reporting process that includes:
    - One point of contact to receive reports of all SGI releases.
    - A numbering system to track the number of releases reported in a consistent manner.
    - A system to report information on releases from the central point of contact to the responsible program offices.
    - A system to trend releases and to make any needed programmatic changes.

2. Update the affected MDs (3.4, 7.4, 12.1, 12.5, and 12.7) to provide consistent guidance on the new reporting structure outlined in recommendation 1.

3. Develop and implement interim guidance to communicate the structured reporting process to NRC staff.

4. Update the annual online security information training to reflect the reporting requirements for SGI releases.

5. Update MD 12.7 to include detailed guidance on granting "outsiders" access to SGI.

6. Develop and issue interim guidance covering how to grant "outsiders" access to SGI.

7. Develop and implement formal business processes for certified designators and the SLES designator role. These procedures should include periodically verifying:
    - The need for individuals to maintain designator role.
    - A match between the certified designator list and the SLES designator user list.

8. Develop and require annual refresher training for the SGI Designator role.

V. AGENCY COMMENTS

At an exit conference on March 28, 2012, agency management stated their general 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 assess if NRC adequately ensures the protection of SGI.

SCOPE

The audit focused on reviewing the policies and procedures currently in place to protect SGI. We conducted this performance audit at NRC headquarters from September 2011 through January 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

The audit team reviewed relevant criteria, including the Code of Federal Regulations, Title 10, Part 73, Section 22, "Protection of Safeguards Information: Specific Requirements"; the Atomic Energy Act of 1954, as Amended, Section 147, "Safeguards Information"; Management Directive 12.7, "NRC Safeguards Information Security Program"; Management Directive 12.5, "NRC Automated Information Security Program"; Management Directive 12.2, "NRC Classified Information Security Program"; Management Directive 12.1, "NRC Facility Security Program"; DG-SGI-1, "Designation Guide for Safeguards Information, Criteria and Guidance"; and SGI Inspection Procedures 71130.06, 81810, and 87135. OIG auditors also reviewed the previous NRC OIG audit report, OIG-04-A-04, "Audit of NRC's Protection of Safeguards Information."

Auditors reviewed all three modules of the SGI designator training course, as well as the Annual Information Security Awareness Course.

At NRC headquarters, in Rockville, Maryland, auditors interviewed NSIR, ADM, Office of the General Counsel, CSO, OIS, and Office of International Programs staff and/or management to gain an understanding of their roles and responsibilities related to the SGI program. Auditors conducted

telephone interviews with 46 NRC staff, at headquarters and the four regional offices, who were on the SGI designator list.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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