OFFICE OF
THE INSPECTOR GENERAL

U.S. NUCLEAR
REGULATORY COMMISSION

Audit of NRC's Protection of Safeguards Information

OIG-04-A-04 January 8, 2004

AUDIT REPORT

All publicly available OIG reports (including this report) are accessible through NRC's website at:
http://www.nrc.gov/reading-rm/doc-collections/insp-gen/

January 8, 2004

MEMORANDUM TO: William D. Travers
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC's PROTECTION OF SAFEGUARDS
INFORMATION (OIG-04-A-04)

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

The report reflects the results of our audit to assess the U.S. Nuclear Regulatory Commission's (NRC) process for protecting safeguards information (SGI). Overall, we found that NRC's use of SGI contains similarities to the Government-wide program to protect confidential information. In light of the events of September 11, 2001, and a subsequent Executive Order redefining confidential information, NRC should determine whether the SGI designation is still justified.

NRC also needs to take strong action to limit inappropriate releases. Specifically, the agency needs clear guidance on what constitutes SGI information and a central program authority to maintain a sound and effective SGI program. The report also identifies concerns with the secure telecommunications network that is used to transmit SGI information. Until the SGI program is strengthened, the likelihood of releasing SGI to unauthorized individuals will remain high.

Comments provided at the September 9, 2003, exit conference, during subsequent discussions, and in a December 12, 2003, written response to the draft report have been incorporated, as appropriate, in our final report. Appendix B contains the written response in its entirety. Appendix C contains our point-by-point analysis of the agency's formal comments.

If you have any questions, please call Russ Irish at 415-5972 or me at 415-5915.

Attachment: As stated

cc: W. Dean, OEDO

R. McOsker, OCM/RAM
B. Torres, ACMUI
B.J. Garrick, ACNW
M. Bonaca, ACRS
J. Larkins, ACRS/ACNW
P. Bollwerk III, ASLBP
K. Cyr, OGC
J. Cordes, OCAA
E. Merschoff, CIO
J. Funches, CFO
P. Rabideau, Deputy CFO
J. Dunn Lee, OIP
D. Rathbun, OCA
W. Beecher, OPA
A. Vietti-Cook, SECY
W. Kane, DEDH/OEDO
C. Paperiello, DEDMRS/OEDO
P. Norry, DEDM/OEDO
M. Springer, ADM
J. Dyer, NRR
G. Caputo, OI
P. Bird, HR
C. Kelley, SBCR
M. Virgilio, NMSS
S. Collins, DEDR
A. Thadani, RES
P. Lohaus, STP
F. Congel, OE
M. Federline, NMSS
R. Zimmerman, NSIR
R. Wessman, IRO
H. Miller, RI
L. Reyes, RII
J. Caldwell, RIII
B. Mallett RIV
OPA-RI
OPA-RII
OPA-RIII
OPA-RIV

EXECUTIVE SUMMARY

BACKGROUND

The definition of safeguards information (SGI) is derived from Section 147 of the Atomic Energy Act of 1954, as amended. It deals with information related to the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material. The U.S. Nuclear Regulatory Commission (NRC) carries out the Act through the Code of Federal Regulations and management directives to ensure that SGI is handled appropriately and is protected from unauthorized disclosure.

PURPOSE

The Office of the Inspector General (OIG) conducted this audit to determine whether NRC adequately defines what constitutes safeguards information, ensures its protection, and prevents its inappropriate release to individuals who should not have access to it.

RESULTS IN BRIEF

NRC has the authority, under the Atomic Energy Act, to establish an SGI program. However, OIG identified the following weaknesses in the SGI program:

❑ The benefit of the SGI designation as sensitive unclassified information is not clear.

❑ Examples in which NRC and licensee representatives inappropriately released SGI to unauthorized individuals.

❑ NRC does not have a central authority for controlling, coordinating and communicating SGI program requirements.

A. SAFEGUARDS DESIGNATION MAY NOT BE NEEDED

NRC's SGI program contains similarities to the Government-wide program to protect confidential information. As such, the benefits of maintaining a separate program are not clearly justified in relation to the cost. Moreover, the agency recently established a SGI-Modified Handling (SGI-M) designation that requires some SGI information to be handled similarly to official use only information. As a result, the agency now has two classes of SGI for marking protected information, both of which appear similar to other programs. Yet, NRC has determined neither the cost of maintaining nor the benefit derived from these separate programs. Without this kind of data, no one knows whether the SGI program should continue or be subsumed under the government-wide program.

B. INAPPROPRIATE RELEASE OF SAFEGUARDS INFORMATION

Recent inappropriate releases of SGI occurred because of handling errors and differing interpretations of what constitutes SGI. The agency is currently reviewing the requirements related to SGI to ensure that the appropriate protections are in place and that the requirements and guidance are clear. In addition, at the time of this report, agency officials were developing a guidance document to describe SGI clearly. However, until adequate tools and training are provided to help with the correct designation and handling of SGI, the likelihood of releasing SGI to unauthorized individuals remains. In effect, NRC has an SGI program that some users do not understand or do not know how to handle the SGI material.

C. NO CENTRAL PROGRAM AUTHORITY FOR PROTECTING SGI

NRC controls do not ensure the protection of SGI because the agency lacks a strong, coordinated SGI program. SGI responsibilities are split between various agency offices and no entity controls the overall SGI program. This decentralization of authority has resulted in (1) inadequate training to identify, handle and distribute SGI, (2) insufficient coordination of the acquisition of secure telecommunications equipment, (3) inadequate installation, maintenance and testing of that equipment, (4) uncoordinated planning for automated processing of SGI, and (5) flawed guidance on the use of LAN-based computers to process SGI.

RECOMMENDATIONS

The consolidated list of recommendations to the Executive Director for Operations is on page 17.

AGENCY COMMENTS

The Deputy Executive Director for Homeland Security and Preparedness stated that NRC has made significant strides in improving the protection of SGI by NRC employees and licensees subsequent to the events of September 11, 2001. Overall, he believes that the SGI program is fulfilling its intended function. However, he also acknowledges that improvements can be made to the program and essentially agrees with the report's recommendations. The Deputy Executive Director's major concern centers on the continued justification for an SGI program vis-a-vis the national classified information system. He specifically believes that it would not be an appropriate use of the NRC staff's time and resources to conduct a cost-benefit study to justify the SGI designation. He asked that OIG look at the wording of this recommendation to assure that it accurately captures the OIG intent. The Deputy Executive Director also provided detailed comments on the draft report for OIG consideration. (See appendix B for a copy of the comments provided by the Deputy Executive Director.)

OIG ANALYSIS OF AGENCY COMMENTS

The primary issue to OIG is whether continuing the SGI designation is justifiable on its merits. During the course of this audit, the primary justification provided by NRC staff for maintaining the SGI designation was the cost associated with doing away with the designation and using the confidential designation in its place. Furthermore, the more detailed comments to the draft report provided by the Deputy Executive Director continued to discuss the costs associated with eliminating the SGI designation.

OIG has reworded its initial recommendation to ensure that NRC formally documents the justification for continued use of the SGI designation. The justification could take several forms, such as a formal legal opinion that SGI is required based on congressional or presidential direction, or it could be justified on the basis of cost of maintaining the current SGI designation vis-a-vis the cost of using the confidential designation. During the audit, NRC staff was not able to provide any formal justification for the SGI designation other than anecdotal accounts of the significant cost involved if it were to change or that it has been done this way for the last 20 years. The issue for OIG is whether, in light of the events of September 11, 2001, and a subsequent Executive Order redefining confidential information, business as usual is still justified. (See appendix C for detailed OIG analysis of the Deputy Executive Director's comments.)

[Page intentionally left blank.]

ABBREVIATIONS AND ACRONYMS

ADM	Office of Administration
AEA	Atomic Energy Act
CFR	Code of Federal Regulations
COMSEC	Communications Security
EDO	Executive Director for Operations
Fax	Facsimile machine
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MD	Management Directive
NMSS	Office of Nuclear Materials Safety and Safeguards
NRC	U. S. Nuclear Regulatory Commission
NRR	Office of Nuclear Reactor Regulation
NSA	National Security Agency
NSIR	Office of Nuclear Security and Incident Response
NUREG	NRC technical report designation
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
RIS	Regulatory Issue Summary
SGI	safeguards information
STE	Secure Terminal Equipment
STU-III	Secure Telephone Unit

[Page intentionally left blank.]

TABLE OF CONTENTS

APPENDIX

[Page intentionally left blank.]

I. BACKGROUND

Based on a congressional request, the Office of the Inspector General (OIG) conducted an audit and issued a report on the U.S. Nuclear Regulatory Commission's (NRC) handling and marking of sensitive unclassified information[1]. The objective of that audit was to assess NRC's program for handling, marking, and protecting one category of sensitive unclassified information — official use only. During that audit, an NRC Commissioner raised concerns about whether NRC staff clearly understood what constitutes safeguards information, another category of sensitive unclassified information. As a result, OIG initiated a follow-on audit concerning the protection of safeguards information.

Derivation of Safeguards Information

The definition of safeguards information (SGI) is derived from Section 147 of the Atomic Energy Act (AEA) of 1954, as amended. It deals with information related to the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material. The AEA states that SGI identifies a licensee's or applicant's detailed:

- Control and accounting procedures or security measures for the physical protection of special nuclear material;
- Security measures for the physical protection of source material or byproduct material; and,
- Security measures for the physical protection of and the location of certain plant equipment.

NRC Internal Controls for Safeguards Information

Following the AEA, NRC developed regulations to prevent the unauthorized disclosure of SGI. NRC stipulated licensee requirements for protecting safeguards information in Title 10 of the Code of Federal Regulations, Part 73, *Physical Protection of Plants and Materials*, Section 73.21, (10 CFR 73.21).

SGI is part of NRC's Sensitive Unclassified Information security program. Sensitive unclassified information consists of information designated as safeguards, official use only, and proprietary. It also includes unclassified information received from other sources (e.g., Government agencies, contractors, licensees) and requires special protective measures.

[1] OIG-03-A-01, *Review of NRC's Handling and Marking of Sensitive Unclassified Information*, October 16, 2002.

Management Directive and Handbook (MD) 12.6, *NRC Sensitive Unclassified Information Security Program*, provides staff requirements to protect SGI. These requirements state that SGI:

- must be communicated over secure telecommunications equipment;
- must not be processed on the local area network (LAN);
- must be properly marked; and,
- must include a cover sheet to facilitate its recognition.

II. PURPOSE

OIG performed this audit to determine whether NRC adequately:

- ♦ defines SGI;
- ♦ prevents the inappropriate release of SGI to anyone who should not have access to it; and,
- ♦ ensures the protection of SGI.

Appendix A provides a detailed description of the audit's scope and methodology.

III. FINDINGS

NRC has the authority, under the Atomic Energy Act, to establish an SGI program. However, OIG identified the following weaknesses in the SGI program:

- ❏ The benefit of the SGI designation as sensitive unclassified information is not clear.
- ❏ Examples in which NRC and licensee representatives inappropriately released SGI to unauthorized individuals.
- ❏ NRC does not have a central authority for controlling, coordinating and communicating SGI program requirements.

A. SAFEGUARDS DESIGNATION MAY NOT BE NEEDED

NRC's SGI program contains similarities to the government-wide program to protect confidential information. As such, the benefits of maintaining a separate program are not clearly justified in relation to the cost. Moreover, the agency recently established a SGI-Modified Handling (SGI-M) designation that requires some SGI information to be handled similarly to official use only information. As a result, the agency now has two classes of SGI for marking protected information, both of which appear similar to other programs. Yet, NRC has determined neither the cost of maintaining nor the benefit derived from these separate programs. Without this kind of data, no one knows whether the SGI program should continue or be subsumed under the government-wide program.

Background

According to an NRC official, early in the agency's history, NRC recognized the need to protect particular information related to nuclear topics that were not classifiable under the National Security Information regime. Consequently, NRC instituted a category of Sensitive But Unclassified information known as "Safeguards Information" under Section 147 of the Atomic Energy Act. As a result, the NRC has a 20-year history of protecting sensitive nuclear information that does not meet the criteria for classification as National Security Information.

Definition of Confidential vs. Safeguards Information

Executive Order 12958, *Classified National Security Information*[2], defines confidential information as that which "the unauthorized disclosure of which reasonably could be expected to cause damage to the national security." [Section 1.2. (a)(3)]

One classification category to which confidential can be applied is:

> vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism. [Section 1.4. (g)]

The various departments and agencies of the Federal Government classified approximately 23.7 million documents in FY 2002. The definition of classified document is understood and is standardized across the Government.

SGI is defined as information related to the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material. NRC is the only agency that uses the SGI designation. Although there is no empirical data, NRC officials estimate that there may be a few thousand SGI documents.

[2] As amended by Executive Order 13292 dated March 25, 2003.

Handling of Safeguards Information vs. Confidential Information

According to NRC's *"Minimum Requirements for Handling Classified and Sensitive Unclassified Information,"* confidential information and SGI are handled similarly.

Category of Information	Transmission Outside NRC	Control Records	Storage	Reproduction Authority	Cover Sheet	Access Authorization	Classification Designation Authorities
CONFIDENTIAL	Certified Mail	Optional	Approved Security Container	As Needed Unless Prohibited by Originator	Yes	"L" and Need-to-Know	Authorized Classifier
SGI	First Class Mail	No	Bar Lock File Cabinet	As Needed	Yes	Need-to-Know	NRC Section Chiefs and Above

As can be seen in the chart, SGI is handled like confidential information, with some lighter restrictions. OIG believes the additional cost of protecting confidential information is minor (e.g., sending documents by certified mail instead of first class or the cost of an approved security container instead of a bar lock). Thus, the cost of maintaining the SGI designation (e.g., the cost of maintaining the regulations, training, etc.) could be more than the additional costs of protecting confidential information.

Handling of Safeguards Modified Information vs. Official Use Only Information

While safeguards and security information at nuclear reactor sites licensed by NRC are handled as SGI, the agency recently notified certain materials licensees that they could use the designation "Safeguards Information-Modified Handling (SGI-M)." Although civil and criminal penalties applicable to SGI apply to unauthorized disclosures of SGI-M, the handling of SGI-M is more relaxed -- more like Official Use Only information.

Category of Information	Transmission Outside NRC	Control Records	Storage	Reproduction Authority	Cover Sheet	Access Authorization	Classification Designation Authorities
OFFICIAL USE ONLY	First Class Mail	No	See 1. Below	As Needed	Yes	Need-to-Know	Originator
SGI-M	First Class Mail	No	See 2. Below	As Needed	Yes	Need-to-Know	NRC Section Chiefs and Above

1. Official use only information stored in NRC space with approved electronic access control or NRC contract guards require no additional physical security measures.

2. SGI-M stored in licensee space must be stored in a locked file drawer or container. SGI-M stored in NRC space must be protected in the same manner as regular SGI information (e.g., bar-lock file cabinets).

Additionally, materials licensees may produce or process SGI-M information on an automatic data processing system requiring the use of entry codes or passwords, without the use of a standalone computer.

Additional Considerations

Agency officials pointed out that additional requirements would be necessary to change the SGI designation from sensitive unclassified information to classified information. One such requirement would be the need for security clearances for licensee employees. They also said that this action would require additional costs and increase the length of time to hire a new employee. Agency officials have differing opinions on the costs licensees would incur with a change in the designation of SGI. One agency official estimated additional costs of $10,000,000 to the industry, based on an average of 500 employees per site at a cost of $200 per employee (actual Government cost is $145 per employee). Another estimated costs to the industry of $14,372,000, based on the same per employee cost, but using an average of 838 employees per site. Licensees stated that current industry costs associated with obtaining criminal checks, fingerprint checks, psychological evaluations and other tests to bring on a new employee average $486.

OIG believes that the requirements to bring new employees onto licensee sites are basically the same as those associated with obtaining appropriate security clearances for having access to confidential information. If licensees were to use NRC as the vehicle for their security checks, new employees would be properly vetted and receive a Government security clearance for about $145, a cost savings to the licensees. However, no one has conducted an in-depth evaluation of the benefit of the current safeguards program as compared to the additional cost, if any, of using the Government-wide confidential designation.

Summary

Especially in the aftermath of the terrorist attacks on September 11, 2001, the OIG questions whether the designation of SGI as sensitive unclassified information is justified or cost effective. OIG believes SGI information can be protected by the standard confidential classification with little or no additional cost. Moreover, SGI-M can be adequately protected by the standard official use only designation.

Agency Comment and OIG Response

In his comments responding to the final draft report (see Appendix B), the Deputy Executive Director for Homeland Security and Preparedness indicated his major concern centers on the continued justification for an SGI program vis-a-vis the national classified information system. He specifically believes that it would not be an appropriate use of the NRC staff's time and resources to conduct a cost-benefit study to justify the SGI designation. He asked that OIG look at the wording of this recommendation to assure that it accurately captures the OIG intent.

The primary issue to OIG is whether continuing the SGI designation is justifiable on its merits. As a result, OIG has reworded its initial recommendation to ensure that NRC formally document the justification for continued use of the SGI designation. The justification could take several forms, such as a formal legal opinion that SGI is required based on congressional or presidential direction, or it could be justified on the basis of the cost of maintaining the current SGI designation vis-a-vis the cost of using the confidential designation.

RECOMMENDATION

OIG recommends that the Executive Director for Operations:

1. Formally document the justification for continued use of the safeguards information designation.

B. INAPPROPRIATE RELEASE OF SAFEGUARDS INFORMATION

Recent inappropriate releases of SGI occurred because of handling errors and differing interpretations of what constitutes SGI. The agency is currently reviewing the requirements related to SGI to ensure that the appropriate protections are in place and that the requirements and guidance are clear. In addition, at the time of this report, agency officials were developing a guidance document to describe SGI clearly. However, until adequate tools and training are provided to help with the correct designation and handling of SGI, the likelihood of releasing SGI to unauthorized individuals remains. In effect, NRC has an SGI program that some users do not understand or do not know how to handle the SGI material.

Background

The definition of SGI is provided within the Atomic Energy Act (AEA), the Code of Federal Regulations, agency management directives, and other agency guidance. However, the definition of SGI results in instances of differing interpretations.

Differences in the Interpretation of Safeguards Information Between Licensees and NRC

Licensees and NRC staff have different interpretations for applying the SGI designation. OIG interviewed NRC resident inspectors[3] and licensee security officials at 15 commercial nuclear power plant sites and 6 nuclear research and test reactor facilities to try to understand these differences.

Licensee officials generally stated that the guidance for applying SGI was not clear, there are inconsistencies in the guidance, and that over the years NRC staff has imposed self-interpretations for SGI. A specific area of confusion is the information included in licensees' weekly security force reports issued for each commercial nuclear power plant to NRC. Resident inspectors and licensee security officials stated that licensees do not believe the information provided for the weekly security force report is SGI, yet NRC designates this as SGI.

Inappropriate Releases of SGI

Weaknesses in the SGI program are further evidenced by inappropriate releases of SGI in documents and on public websites. One licensee presented a contingency plan to Region IV that the licensee believed was cleansed of SGI. The report made it through two licensee revisions without any identification that it contained SGI. On its third revision, an NRC official determined the report contained SGI. By this time, the licensee had shared the contingency plan with local law enforcement and had to collect it back from them. In another instance, a licensee prepared a presentation with pictures that compromised the security of a commercial nuclear power plant. Originally, NRC expressed no concerns that the presentation contained SGI and included it on the agency's website. It was not until an NRC headquarters official determined that the presentation included SGI that the agency removed the presentation from the website.

Recent events involving NRC employees provide further evidence of weaknesses in control and handling of SGI.

❑ An NRC employee distributed a document that contained force-on-force program findings to the public. The employee believed the report was "sanitized" and distributed the report to nuclear industry officials, who then distributed the report to the press. NRC officials later determined that the report contained SGI that had not been properly marked.

[3] For purposes of this report, OIG uses the term " resident inspectors" to denote NRC staff interviewed at commercial nuclear power reactor sites and does not distinguish between resident inspectors and senior resident inspectors.

❑ The release of SGI occurred at an industry-sponsored meeting when a guest NRC speaker mentioned SGI relating to the agency's force-on-force security testing program. However, the SGI had already been publicly available through other sources.

❑ NRC staff made another document related to the force-on-force program, which contained SGI, available to the public on the external NRC website.

A March 2003 NRC release of SGI shows the possible significant consequences of not having adequate controls over this type of information. NRC had developed a Regulatory Issue Summary (RIS) containing agency designated SGI. The RIS was intended for "all power reactor (including decommissioning reactor) licensees, independent spent fuel storage installation licensees, the conversion facility licensee, gaseous diffusion plant licensees, and Category I fuel cycle facility licensees." However, NRC released the RIS not only to the identified groups, but also to Category III fuel cycle facility licensees and certain vendors. According to an NSIR official, this was because one program office provided an inappropriate mailing list that included entities that should not have received the document. This NSIR official added that the staff responsible for the mailing was "junior staff" who did not recognize the inappropriate addresses. To compound the severity of this release, the RIS contained specific information about methods and techniques of defeating physical barriers at nuclear facilities, which would be of value to potential adversaries.

Summary

These examples of inappropriate releases resulted from a combination of handling errors and differing interpretations of what information constitutes SGI. Without clear guidance on how to designate SGI, agency and licensee staff will continue to release SGI to unauthorized individuals inappropriately. The agency is preparing a guidance document to help with the identification of SGI; however, it is not yet complete.

RECOMMENDATION

OIG recommends that the Executive Director for Operations:

2. Finalize and issue the safeguards information designation guidance document currently being developed.

C. NO CENTRAL PROGRAM AUTHORITY FOR PROTECTING SGI

NRC controls do not ensure the protection of SGI because the agency lacks a strong, coordinated SGI program. SGI responsibilities are split between various agency offices and no entity controls the overall SGI program. This decentralization of authority has resulted in (1) inadequate training to identify, handle and distribute SGI, (2) insufficient coordination of the acquisition of secure telecommunications equipment, (3) inadequate installation, maintenance and testing of that equipment, (4) uncoordinated planning for automated processing of SGI, and (5) flawed guidance on the use of LAN-based computers to process SGI.

Background

Aspects of the SGI program are split among the NRC's Offices of Administration (ADM), Nuclear Security and Incident Response (NSIR), the Chief Information Officer (OCIO), Nuclear Material Safety and Safeguards (NMSS), and Nuclear Reactor Regulation (NRR). While NRC has a single agency official for homeland protection and preparedness issues, SGI protection controls are fragmented. As a result, there is no central authority for the agency's SGI program and no single organization controls the program.

Distribution of SGI Responsibilities

	ADM	NSIR	OCIO	NMSS	NRR
Inform Licensees of Guidance				√	√
Training NRC Employees	√	√	√		
Computer Processing			√		
Secure Telephones		√			
ISDN Lines[4]			√		
Requirements Information[5]	√				

NRC has invested more than $600,000 to provide secure telecommunications equipment in headquarters, the four regional offices, and at all resident inspector offices. The agency did this to ensure the agency could send classified information to the licensees. The Commission believed that licensees were entitled to the information necessary to evaluate the threats to their plants and to defend their facilities. This policy resulted in an exponential growth in the secure telecommunications equipment for which the agency is responsible. NRC acquired Secure Terminal Equipment (STE)[6] for use at headquarters and the regional offices. The agency also distributed older Secure Telephone Units -

[4] The Integrated Services Digital Network is a high speed digital communication network.

[5] Minimum Requirements for Handling Classified and Sensitive Unclassified Information.

[6] The STE is secure voice and data equipment designed for use on digital communications networks, although they can operate in the analog mode.

Model 3 (STU-III)[7](previously possessed by NRC or provided by the U.S. Army) to resident inspector offices at commercial nuclear power reactor sites. NRC also purchased secure fax machines to be connected and used jointly with the secure telephones.

STE

Equipment	*Number*	*Cost*
STE	94	$370,000
STU-III	71	-0-
Secure Fax	78	$242,000
TOTAL		$612,000

In addition, licensees will pay more than $45,000 for security clearances to allow direct communication with NRC officials over the secure telecommunications equipment in the resident inspector offices. NRC directed that five licensee representatives at each site receive a security clearance[8]. To obtain each clearance, licensees pay NRC a fee of about $145 for each security clearance, or $725 per site for 65 sites.

Inadequate Training

Training related to SGI is fragmented. There is no single point of ownership for training on handling and protecting information among the program offices. NMSS officials stated that, while they are not responsible for training other NRC employees and contractors, they do provide training for their own staff. ADM officials stated they stopped providing training in information security areas for NRC employees and contractors since the creation of NSIR. However, ADM does give NRC employees certain types of security education, programs and security awareness tools.

Before June 2003, NRC had not provided agency-wide SGI training to agency employees. Some program offices within NRC headquarters requested training on the handling of sensitive unclassified information and received it within the past year. The same is true for all four of NRC's regional offices. However, not all employees involved with or responsible for controlling SGI had received formal documented training. In response to OIG's previous audit report on the handling and marking of sensitive unclassified information, NSIR agreed to develop a comprehensive security education program for handling both classified and sensitive unclassified information that includes SGI. NRC completed this training for agency employees in July 2003.

[7] The STU-III is a secure analog telephone unit that can encrypt voice and data communications worldwide.

[8] Licensee representatives will receive an 'L' security clearance based on a national agency check with inquiries.

Acquisition of Secure Telecommunications Equipment

An additional benefit of secure telecommunications equipment is using it to transmit SGI. ADM had responsibility for the FY 2002 installation of secure telecommunication equipment in the resident inspector offices at commercial nuclear power plants. During this period, ADM also was the Central Office of Record[11] for the agency. NRC got the equipment expeditiously because of the concerns of additional terrorist attacks. After NSIR was established, ADM's duties were transferred to that office.

NSIR will need to consult with OCIO to install ISDN lines to operate secure telephone equipment because OCIO controls the acquisition and installation of ISDN lines. This collaboration between OCIO and NSIR will be integral for making decisions about future alternatives to the secure telephones. For example, National Security Agency (NSA) officials told OIG that new equipment is now available that can encrypt conversations through regular telephones. This is possible without the use of special equipment, such as STU-IIIs or STEs, or an ISDN line. As a result, NRC needs to coordinate future secure telecommunications equipment purchases among responsible offices to ensure that appropriate equipment is obtained.

Inadequate Installation, Maintenance, and Testing of Secure Equipment

Installation

Agency requirements state that secure telecommunications equipment that is newly installed, moved, or modified must not be operated until ADM has done the required security checks. ADM-authorized qualified maintenance personnel also must determine that the equipment is properly installed with all required modifications and ready for operation. These requirements were written (1) when very few secure telephones existed, (2) when the secure telephones were mostly in headquarters and the regional offices, and (3) before NSIR assumed the responsibilities of ADM for these activities. While these requirements are still applicable today, they were not followed when the agency installed the new secure telecommunications equipment in the resident inspector offices. Agency officials said that OCIO had previously provided one person whose primary responsibility was to visit headquarters and regional office sites where secure telecommunications equipment was found and provide technical services. However, while installing the new STEs, OCIO provided assistance for configuring ISDN lines, which were primarily installed at headquarters.

[11] The Central Office of Record performs oversight of all NRC communications security accounts and coordinates all communications security activities with the National Security Agency for NRC.

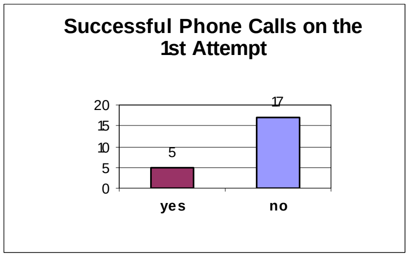
Maintenance

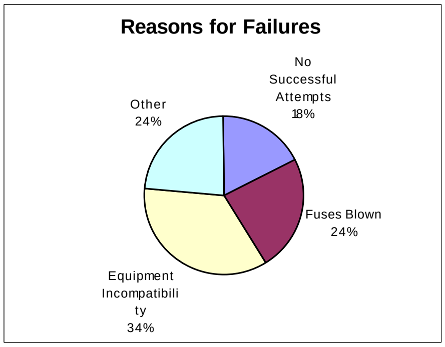
Communications security (COMSEC) custodians[12] are not responsible for the physical maintenance of the secure equipment, although they may be called upon for troubleshooting the operation of that equipment. An OCIO manager stated that COMSEC custodians do not have the technical expertise to maintain the secure equipment. Also, this manager said that OCIO itself did not have the additional technical resources needed to support all of the secure telecommunications equipment. Although NSIR asked regional management to provide COMSEC support for installing and maintaining secure telecommunications equipment, regional management expressed concern that the equipment would require additional resources for which they are not currently budgeted. As such, the agency does not currently provide the necessary resources to visit each site to install and test secure telecommunications equipment.

Testing

OIG directed limited testing of the secure telecommunication system to determine whether it worked as intended and if agency staff were familiar with its operation. Testing determined that NRC's secure telecommunications system may not work when needed and SGI could be compromised.

OIG observed twenty-two tests of the secure telephones and fax machines. Four tests were initiated from NRC headquarters and 18 from the backup Incident Response Operation Center. Seventeen of the tests failed on the first attempt to obtain a secure connection and then receive and subsequently transmit a secure fax transmission. Five of the tests performed properly on the first attempt.





Of the 17 initial failed tests, 5 sites were never able to send or receive a fax. The remaining 12 sites failed due to unsuccessful initial telephone connections, failed fax fuses, or failure of a STU-III to connect with a STE or vice-versa. The other category includes issues such as: a security safe that would not open, which prevented the resident inspector from retrieving the encryption key needed to activate the secure telephone; a caller switching from secure data before the fax transmission was completed; and, two cases when the reasons for failure were indeterminate.

[12] The agency has identified COMSEC custodians within headquarters and at each regional office to provide training to secure telecommunications users in their office or region and perform a semi-annual physical inventory of all secure telecommunications equipment.

NSIR representatives said that, prior to OIG's test, the agency only tested the secure network after the initial installation of the secure telecommunications equipment at each resident inspector office. Furthermore, there were no plans to establish ongoing, periodic testing. Resident inspectors recognized there were operational problems with the secure telecommunications equipment, but they did not appear overly concerned. Some stated that, in an emergency, they would opt to use the regular telephone as management directives provided examples of extraordinary circumstances under which SGI may be discussed over unsecured telephone lines. However, it is NRC's policy to use the secure telecommunications system equipment for the day-to-day transmittal of SGI and classified infomation.

Uncoordinated Planning for Automated Processing of SGI

NRC is considering using encrypted e-mail to transmit SGI. Prior to establishing NSIR, a working group made up of representatives from various NRC program offices and industry representatives discussed the need to electronically transmit SGI. The working group developed NRC RIS 2002-15, *NRC Approval of Commercial Data Encryption Systems for the Electronic Transmission of Safeguards Information*, dated August 28, 2002. This document provides guidance on obtaining agency approval of commercial data encryption systems for the electronic transmission of SGI.

To develop a viable electronic transmission and processing program for SGI, agency officials will need to work collaboratively. While OCIO is responsible for computer processing, ADM is responsible for access authorization, NSIR for information security, and NMSS and NRR for providing guidance to the licensees. Although all of these offices concurred in the development of NRC RIS 2002-15, no single office has overall authority to coordinate and control the program to ensure consistency of effort, economy and efficiency in application.

Technically Flawed Guidance for Computer Processing of SGI

NRC guidance on processing SGI on computers is technically flawed. NUREG/BR-0168, Revision 2[13] allows the use of a LAN-based computer for processing SGI as long as the computer is disconnected from the LAN prior to its use in processing SGI. However, NSA officials stated that this method places a shadow file on the hard drive of the computer, which then could be accessed through the LAN when the computer is reconnected. NSA studies found traces of classified documents on hard drives even though documents were processed using floppy disks. In short, SGI should not be processed on any computer that is or will be connected to the LAN.

[13] NUREG/BR-0168, Revision 2 *Policy for Processing and Handling Unclassified Safeguards Information and Other Sensitive Information in the NRC Local-Area /Wide-Area Network Environment*, December 1999.

Summary

In order for NRC to maintain a sound and effective SGI program, it must be managed by a central authority. That authority should have the ability to engage resources throughout the agency and be able to hold them accountable for the tasks at hand. In addition, a central authority would be able to ensure a consistent application of SGI guidance and training, and maintain oversight for secure telecommunications equipment and automated processing of SGI. While NRC has a single agency official for homeland protection and preparedness issues, there is no central authority for the agency's SGI program.

NRC has invested more than $600,000 in secure telecommunications equipment for a classifed information and SGI (sensitive unclassified) program that is not working as intended. The amount of secure telecommunications equipment currently within the agency has outgrown NRC's resources to provide adequate installation, oversight, and maintenance of that equipment. The agency needs to perform regular, documented tests to ensure that the secure telecommunications network is operating properly and that NRC staff is familiar with its operation. Additionally, agency guidance on computer processing of SGI must clearly indicate that the use of a LAN-based system is prohibited.

RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

3. Designate a central authority for controlling, communicating and coordinating the safeguarrds information program.

4. Provide adequate resources to ensure the timely installation, maintenance, and troubleshooting of problems with secure telecommunications equipment.

5. Formalize a program for periodic testing and documentation of the secure telecommunications network.

6. Revise NRC procedures to eliminate the processing of SGI on the LAN.

IV. NRC MANAGEMENT INITIATIVES

NSIR is making progress on corrective actions in answer to the recommendations made in the recently issued OIG audit report on the handling and marking of sensitive unclassified information. Specifically, the office is conducting a total review of MD 12.6 to make the guidance more prescriptive and is developing a security education program. This program will be used for training NRC employees and contractors about the handling of both classified and unclassified sensitive information.

On May 20, 2003, NSIR issued a Yellow Announcement reminding agency staff of the requirement to report inadvertent releases to the EDO and the OIG. The announcement also notified agency staff of available monthly training concerning the protection and handling of classified and sensitive unclassified information. NSIR also conducted mandatory security classes in June and July 2003, in response to recommendations made in OIG's earlier audit report. After that, NSIR will continue to provide monthly training sessions at the request of the program offices, as long as there are at least 5 to 10 individuals that need the training. Although NSIR is taking actions to strengthen the controls over sensitive unclassified information, OIG believes that the information and recommendations contained in this report must be factored into any revised training program NSIR develops.

The cover sheets for classified information and SGI were modified to include instructions on the proper handling of documents containing these types of information. The cover sheet for SGI was changed from green to purple to better distinguish it from the Official Use Only cover sheet, which is green and white. Instructions for marking, storing, handling and transmitting SGI are included on the reverse side of the cover sheet to provide users with a quick reference guide on handling and protecting SGI. The requirement for the use of secure telecommunications equipment is also highlighted for the electronic transmission of SGI. Having the guidance on the cover sheet provides information to those employees who do not often handle SGI, and provides a quick refresher for those who are more familiar with the requirements. Effective May 15, 2003, agency personnel were requested to cease using the green version of the SGI cover sheet and begin using the purple cover sheet.

Although NRC implemented a plan in June 2002 for the comprehensive review of safeguards and security programs for NRC-licensed facilities and activities, it has yet to complete the actions designated in that plan. Of particular interest to the subject of this report, the agency has not completed its review of the requirements related to SGI. The recommendations contained in this report must be factored into any further implementation and completion of that plan.

[Page intentionally left blank.]

V. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Formally document the justification for continued use of the safeguards information designation.

2. Finalize and issue the safeguards information designation guidance document currently being developed.

3. Designate a central authority for controlling, communicating and coordinating the safegurards information program.

4. Provide adequate resources to ensure the timely installation, maintenance, and troubleshooting of problems with secure telecommunications equipment.

5. Formalize a program for periodic testing and documentation of the secure telecommunications network.

6. Revise NRC procedures to eliminate the processing of SGI on the LAN.

[Page intentionally left blank.]

APPENDIX A

SCOPE AND METHODOLOGY

OIG audited the protection of safeguards information at NRC. To accomplish the audit objectives, OIG reviewed NRC Management Directives, agency guidance, OIG reports, and outside agency documents. Auditors interviewed NRC employees, licensee security officials, Department of Energy employees, and representatives from the National Security Agency to determine their understanding of the SGI definition, familiarity with the operation of the secure telecommunication equipment and practices for protecting SGI. OIG performed tests of the secure telephones and fax machines located at Regions I and IV and 22 different resident inspector sites.

The work was conducted from October 2002 through April 2003 in accordance with generally accepted Government auditing standards and included a review of management controls related to the objectives of the audit.

The major contributors to this report were: Russell Irish, Team Leader; Shyrl Coker, Audit Manager; David Ditto, Management Analyst; and William Kemper, Technical Advisor.

[Page intentionally left blank.]

APPENDIX B

AGENCY COMMENTS

December 12, 2003

MEMORANDUM TO: Stephen D. Dingbaum
Assistant Inspector General for Audits

FROM: William F. Kane **/RA/**
Deputy Executive Director for Homeland
Protection and Preparedness
Office of the Executive Director for Operations

SUBJECT: OIG DRAFT REPORT: AUDIT OF NRC'S PROTECTION OF SAFEGUARDS INFORMATION

This memorandum is in response to your memorandum dated October 28, 2003, forwarding the Office of the Inspector General's (OIG's) draft audit report entitled "Audit of NRC's Protection of Safeguards Information" for staff review and comment. There has been more extensive interaction between OIG and NRC staff regarding this draft report which has led to an unusual delay in my providing you this response.

After receipt of the draft report in August 2003, the staff had several issues with the conclusions reached by OIG, including some of the facts on which those conclusions were based. Of particular concern were two items: (1) the broad conclusion reached regarding the staff's control of safeguards information (SGI) and (2) the recommendation that the staff perform a cost-beneficial analysis to justify the continued use of SGI. Comments on the draft report, which focused heavily on the above two items, were provided to you and your audit team during both a teleconference and a subsequent exit conference in early September 2003. Additionally, there have been several follow-up interactions between OIG and the NRC staff to further our understanding of the basis for OIG's conclusions and recommendations, as well as better explain the NRC staff's concerns with the draft report. It is my understanding that this has resulted in a number of changes that will be reflected in the final report. I appreciate the willingness of the OIG to remain open to the feedback provided by the staff.

Regarding the OIG recommendation that NRC perform a cost-benefit study relative to sustaining the SGI designation, it is my understanding that the OIG's intent is that the staff evaluate if alternatives to the current SGI program are warranted vice doing a formal cost-benefit analysis. Given its clear statutory role, the lack of a reasonable alternative, and its current role in providing an essential information designation and protection system, doing such a cost-benefit analysis would not be an appropriate use of the NRC staff's time and resources. I would ask you to look at the wording of this recommendation to assure that it accurately captures the OIG intent.

The OIG has identified several areas in which the current SGI program can be improved, and we essentially agree with these recommendations. Overall, however, the SGI program is fulfilling its intended function of protecting sensitive security information related to nuclear facilities. I also believe the NRC has made significant strides in improving the protection of SGI by NRC employees and licensees over the past several years subsequent to the events of 9/11.

In addition to the comments above, attached are more detailed comments on the draft report for your consideration. If you would like to discuss our comments, please contact William Dean at 415-1703 or Melinda Malloy at 415-1785.

Attachment: As stated

Comments on OIG Draft Report: Audit of NRC's Protection of Safeguards Information

Page i, Background, states that SGI deals with information related to the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material. This description is correct, but incomplete. Section 147 of the Atomic Energy Act (AEA) also authorizes the Commission to designate as SGI information related to the physical protection of source material and/or byproduct material in quantities determined by the Commission to be significant to the public health and safety or common defense and security. This authority should be noted to correctly reflect the full scope of the Commission's authority under AEA § 147.

Page 1*,* Derivation of Safeguards Information, initially implies that the SGI designation only applies to information related to the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material. Section 147 of the AEA also authorizes the Commission to designate as SGI information related to the physical protection of source material and/or byproduct material in quantities determined by the Commission to be significant to the public health and safety or common defense and security. Although this is noted in a bullet on the same page, the discussion could be clarified up front.

Page 4, first paragraph: There are important differences between the NRC's SGI program and the government-wide program to protect classified national security information (NSI). NSI is subject to more burdensome handling, storage, and access authorization requirements. Requiring NRC licensees to move away from SGI and toward an NSI security clearance and handling regime would impose substantial burdens during the transition and afterwards as private sector employees would be required to undergo more rigorous background checks and training programs to properly receive and handle NSI.

The criteria for classifying information as NSI are different from the criteria for SGI. Eliminating the SGI designation would potentially leave vital information regarding critical security systems, plans, and vulnerabilities unprotected against public disclosure where such information could not be classified under the NSI regime.

Page 5, Definition of Confidential vs. Safeguards Information: The draft report does not justify its assumption that the additional cost of protecting confidential NSI would be minor compared to the cost of protecting SGI. The NRC would have to adjudicate thousands of additional security clearances under an NSI regime and periodically reinvestigate some cleared individuals. NRC would incur additional costs for expanding its infrastructure for performing these tasks. There may also be increased costs to inspect licensees' conformance with regulations for protecting classified information.

Switching from an SGI regime to an NSI regime would not necessarily result in a wholesale elimination of licensees' current programs for evaluating the trustworthiness of its employees because not all licensee employees would require NSI security clearances. The cost of providing the more rigorous background checks required for access to NSI would be in addition to the cost of existing programs, not in substitution of those costs.

Page 6, last paragraph: SGI is not a classification system. There may be additional burdens in the protection of SGI if converted to CONFIDENTIAL-National Security Information which are not reflected in the draft report, e.g., use of security container check sheets and security container information forms posted on the inside of the locking drawer of the container. Security education briefings must be established and conducted (e.g., initial security briefing, refresher briefings every 3 years, and termination briefings) and authorized classifiers will need to be designated and trained on the requirements of Executive Order (E.O.) 12958, as amended. The statement that NRC is the only agency that uses the SGI designation, incorrectly implies that other agencies can meet their needs with the Official Use Only (OUO) and classified designations, with nothing in between. Many other agencies use designations similar in nature (e.g., DOE uses Unclassified Controlled Nuclear Information (UCNI)).

Page 7, Handling of Safeguards Modified Information: The OUO designation is not a useful alternative to the SGI designation. An OUO label does not automatically exempt information from public disclosure under the Freedom of Information Act, as does the SGI designation. Moreover, the OUO designation is not legally binding on NRC licensees. NRC licensees in possession of OUO information are under no legal obligation to provide even the most basic protections. Thus, the OUO designation is not a viable alternative to SGI or SGI-M, both of which attach civil and criminal penalties to unauthorized disclosures and provide a measure of deterrence to unauthorized disclosures.

Page 8: The cost of NRC adjudicating thousands of additional "L" clearances and the cost of periodic reinvestigations have not been considered. In the second paragraph, there is no mention of the 145(b) provision which will need to be adhered to. Not all employees would require Government clearances. Therefore, the licensee would still have to conduct the employee evaluation programs for those not requiring clearances, so the licensee could not necessarily entirely forego the fixed costs of maintaining its own employee evaluation program.

In many cases, the licensee might still have to conduct its own employee evaluation in order to bring an employee on site, and have the Government clearance be granted later. In the interim, an employee would not be permitted to access certain classified information that formerly had been SGI and which does not require a Government clearance for access. This could pose a significant problem for the licensee and could have significant monetary costs, as well as negative safety and safeguards implications.

Should the NRC take on the responsibility for providing Government clearances for large numbers of licensee personnel, NRC would incur additional costs for expanding its infrastructure for performing these tasks. There may also be increased costs to inspect licensees' conformance with regulations for protecting classified information. These expenses would likely be charged to the licensees through NRC's fee recovery process. On balance, licensees could incur significant additional costs, rather than savings.

We suggest that Recommendation 1 be rephrased, as follows:

> "1. Determine whether ~~the benefit of the safeguards information designation is worth the cost of maintaining a separate safeguards program~~ alternatives to the current SGI program, including subsuming SGI under the government-wide program for protecting classified information, could provide more effective and efficient protection against inappropriate release of sensitive information."

Page 10, second paragraph: Different interpretation of what is or is not SGI should not be considered unusual. In classified programs, determining what is classified is not always an exact science. Therefore, different interpretations are always being challenged. It is reasonable to expect the same to hold for the SGI program.

Page 11, first paragraph: Although the SGI that was given to the Local Law Enforcement Agency (LLEA) was not properly marked, the release was not inappropriate because LLEAs are authorized access to SGI in accordance with 10 CFR 73.21.

Page 13, Section C, first paragraph: Items 2 and 3 have nothing to do with a "Central Authority" needed for the oversight of the NRC SGI program. Secure telecommunication equipment acquisition and installation is covered under NRC's classified information program. It should also be noted that while NSIR controls the SGI program as a whole, it still relies on the expertise of the Office of the Chief Information Officer (OCIO) for equipment support, the Office of Administration for physical security oversight, and the Regions and program offices for oversight of licensees handling SGI.

Page 15: Although the equipment may be used to communicate SGI, the purchase of secure communications equipment for NRC resident offices was not done under the aegis of or to support the SGI program.

In the section on Inadequate Training, NSIR has been coordinating training sessions that include the protection and handling of SGI since September 11, 2001. As of August 2003, approximately 90 percent of the agency has been trained on the proper handling requirements for SGI. NSIR has also issued agency announcements, created a cover sheet with handling and marking requirements on the reverse side, and created a new marking stamp that is consistent with current SGI requirements.

Page 16, last paragraph: NSIR has always coordinated with OCIO for the installation of ISDN lines to operate secure telephone equipment and will continue to do so.

Page 18, Maintenance: COMSEC Custodians are responsible for troubleshooting operational problems with secure equipment, rekeying secure telephones, and changing fuses associated with the equipment from time to time. With respect to maintenance, all equipment is required to be sent to a secure maintenance site when repairs are required.

In the section on Testing, it should be noted that the staff considers any use of secure telecommunication equipment to qualify as a test. Problems associated with secure telecommunication are frequently the result of operator error. In addition, many secure connections take several attempts to complete because of the multiplicity of settings possible for each phone and fax. This may even result from the differences in versions of equipment being used.

Page 19, second paragraph: Failure to be able to open a security container is usually due to operator error.

Last paragraph: Secure telecommunications equipment was primarily installed at Reactor Resident Inspector sites for transmission of classified information, not for SGI. If SGI needs to be sent outside a site on a non-emergency basis, it can be done thru U.S. Mail as has been practiced.

Page 20, second paragraph: NSIR has already taken the lead for coordinating and controlling the electronic transmission and processing program for SGI.

Last paragraph: OCIO has already rescinded NUREG/BR-0168, Rev. 2 entitled, "Policy for Processing and Handling Unclassified Safeguards Information and Other Sensitive Information in the NRC Local-Area/Wide-Area Network Environment," to eliminate the processing of SGI on the NRC LAN.

Page 21: The draft report states, "In short, SGI should not be processed on any computer that is or will be connected to the LAN." The report's corresponding Recommendation 6 ("Revise NRC procedures to eliminate the processing of SGI on the LAN") appears to be unnecessarily restrictive.

The draft report highlights an important fact, i.e., that existing guidance for automated processing of SGI is not consistent, and in some cases wrong. This may be addressed in other ways.

We recommend that Recommendation 6 be changed to read:

> "6. Revise documentation for NRC procedures to eliminate ~~the processing of SGI on the LAN~~ inconsistencies and ambiguities that could imply SGI can be processed on a personal computer while it is connected to the unclassified NRC LAN, and to ensure that personal computers used for SGI processing while disconnected from the LAN do not employ fixed hard drives."

Page 22: The report's Recommendations 4 and 5 deal with telecommunications equipment for transmitting SGI. Pages 16 through 19 of the report address acquisition, installation, maintenance, and testing of this equipment, detailing numerous problems with testing and reliability. On page 16, however, there is a statement about the availability of new equipment that can encrypt conversations through regular telephone lines, without the use of special equipment, such as STU-IIIs or STEs, or an ISDN line. The report appeared to encourage a switch to this new technology.

Recommendations 4 and 5 on page 22 seem to neglect this promising new and available technology, and focus instead on continuing to commit resources for the less reliable technology now owned by the NRC. They refer to a separate secure telecommunications network that may not be necessary if the new technology is used. Recommendations 4 and 5 should be revised to permit or encourage a switch to the new technology, rather than force NRC into spending large amounts of money to acquire, install, test, and maintain the current technology that involves supporting a separate secure telecommunications network.

The transition to a new secure telecommunications technology may not be instantaneous or painless, but the report's recommendations should not, in effect, restrict us to staying with the current technology longer than necessary. We suggest the following revisions to Recommendations 4 and 5:

> "4. Provide adequate resources to ~~ensure the timely installation, maintenance, and troubleshooting of problems with~~ acquire, install, test, and maintain appropriate secure communications technology to effectively and efficiently support the secure telecommunications ~~equipment~~ needs of the NRC, as new technologies become available and affordable."

> "5. Formalize a program for periodic testing and documentation of the currently installed secure telecommunications ~~network~~ systems to ensure continuing functionality for regular use and its readiness for emergency use."

[Page intentionally left blank.]

DETAILED OIG ANALYSIS OF AGENCY COMMENTS

Agency Comments:

Page i, Background, states that SGI deals with information related to the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material. This description is correct, but incomplete. Section 147 of the Atomic Energy Act (AEA) also authorizes the Commission to designate as SGI information related to the physical protection of source material and/or byproduct material in quantities determined by the Commission to be significant to the public health and safety or common defense and security. This authority should be noted to correctly reflect the full scope of the Commission's authority under AEA § 147.

OIG Response:

While the agency is correct, the paragraph cited is in the Executive Summary of the report which provides a synopsis of the total report. Page 1 of the report provides a fuller description of SGI.

Agency Comments:

Page 1*,* Derivation of Safeguards Information, initially implies that the SGI designation only applies to information related to the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material. Section 147 of the AEA also authorizes the Commission to designate as SGI information related to the physical protection of source material and/or byproduct material in quantities determined by the Commission to be significant to the public health and safety or common defense and security. Although this is noted in a bullet on the same page, the discussion could be clarified up front.

OIG Response:

OIG agrees that the discussion cited in the bullet *could* be clarified up front, but believes the paragraph and bullets accompanying it are accurate and do not need to be changed.

Agency Comments:

Page 4, first paragraph (now page 2 of this report): There are important differences between the NRC's SGI program and the government-wide program to protect classified national security information (NSI). NSI is subject to more burdensome handling, storage, and access authorization requirements. Requiring NRC licensees to move away from SGI and toward an NSI security clearance and handling regime would impose substantial burdens during the transition and afterwards as private sector employees would be required to undergo more rigorous background checks and training programs to properly receive and handle NSI.

The criteria for classifying information as NSI are different from the criteria for SGI. Eliminating the SGI designation would potentially leave vital information regarding critical security systems, plans, and vulnerabilities unprotected against public disclosure where such information could not be classified under the NSI regime.

Page 5, Definition of Confidential vs. Safeguards Information (now page 3 of this report): The draft report does not justify its assumption that the additional cost of protecting confidential NSI would be minor compared to the cost of protecting SGI. The NRC would have to adjudicate thousands of additional security clearances under an NSI regime and periodically reinvestigate some cleared individuals. NRC would incur additional costs for expanding its infrastructure for performing these tasks. There may also be increased costs to inspect licensees' conformance with regulations for protecting classified information.

Switching from an SGI regime to an NSI regime would not necessarily result in a wholesale elimination of licensees' current programs for evaluating the trustworthiness of its employees because not all licensee employees would require NSI security clearances. The cost of providing the more rigorous background checks required for access to NSI would be in addition to the cost of existing programs, not in substitution of those costs.

Page 6, last paragraph (now page 4, second paragraph of this report): SGI is not a classification system. There may be additional burdens in the protection of SGI if converted to CONFIDENTIAL-National Security Information which are not reflected in the draft report, e.g., use of security container check sheets and security container information forms posted on the inside of the locking drawer of the container. Security education briefings must be established and conducted (e.g., initial security briefing, refresher briefings every 3 years, and termination briefings) and authorized classifiers will need to be designated and trained on the requirements of Executive Order (E.O.) 12958, as amended. The statement that NRC is the only agency that uses the SGI designation, incorrectly implies that other agencies can meet their needs with the Official Use Only (OUO) and classified designations, with nothing in between. Many other agencies use designations similar in nature (e.g., DOE uses Unclassified Controlled Nuclear Information (UCNI)).

Page 8 (now page 5, second paragraph of this report): The cost of NRC adjudicating thousands of additional "L" clearances and the cost of periodic reinvestigations have not been considered. In the second paragraph, there is no mention of the 145(b) provision which will need to be adhered to. Not all employees would require Government clearances. Therefore, the licensee would still have to conduct the employee evaluation programs for those not requiring clearances, so the licensee could not necessarily entirely forego the fixed costs of maintaining its own employee evaluation program.

In many cases, the licensee might still have to conduct its own employee evaluation in order to bring an employee on site, and have the Government clearance be granted later. In the interim, an employee would not be permitted to access certain classified information that formerly had been SGI and which does not require a Government clearance for access. This could pose a significant problem for the licensee and could have significant monetary costs, as well as negative safety and safeguards implications.

Should the NRC take on the responsibility for providing Government clearances for large numbers of licensee personnel, NRC would incur additional costs for expanding its infrastructure for performing these tasks. There may also be increased costs to inspect licensees' conformance with regulations for protecting classified information. These expenses would likely be charged to the licensees through NRC's fee recovery process. On balance, licensees could incur significant additional costs, rather than savings.

We suggest that Recommendation 1 be rephrased, as follows:

> "1. Determine whether ~~the benefit of the safeguards information designation is worth the cost of maintaining a separate safeguards program~~ alternatives to the current SGI program, including subsuming SGI under the government-wide program for protecting classified information, could provide more effective and efficient protection against inappropriate release of sensitive information."

OIG Response:

During the audit, NRC staff was not able to provide any formal justification for the SGI designation other than anecdotal accounts of the costs involved to change it or that it has been done this way for the last 20 years. NRC should formally document that the legal basis for continued use of the SGI designation is justified on its merits alone. Absent that position, the primary anecdotal justification provided by NRC staff for maintaining the SGI designation was the cost of doing away with the SGI designation in order to go to the confidential designation. OIG was provided with this same position during the audit fieldwork, but agency staff could not provide any detailed analysis of the difference in cost between the two designations. In some cases, licensees with whom OIG spoke were implementing actions in protecting SGI which agency staff described as added burdens if the confidential designation was required. OIG attempted to perform a cost-benefit analysis for maintaining the SGI designation, but the figures provided by agency staff and licensees were inconsistent, wide ranging, and non-inclusive for all of the considerations identified by the staff. The point of this finding, in light of the events of September 11, 2001, and a subsequent Executive Order re-defining confidential information, is whether business as usual is still justified.

OIG made minor modifications to the draft report to clarify some of the other points made by the staff. Additionally, OIG reworded the recommendation for this finding to more directly articulate OIG's expectation.

Agency Comments:

Page 10, second paragraph (now page 7, first paragraph of this report): Different interpretation of what is or is not SGI should not be considered unusual. In classified programs, determining what is classified is not always an exact science. Therefore, different interpretations are always being challenged. It is reasonable to expect the same to hold for the SGI program.

OIG Response:

While OIG understands the staff's comments, OIG cannot endorse this position to excuse inappropriate releases of SGI. A clearer definition of SGI can only help to prevent inappropriate releases of SGI and limit the number of occasions where different interpretations have influenced such releases.

Agency Comments:

Page 11, first paragraph (now page 7, third paragraph of this report): Although the SGI that was given to the Local Law Enforcement Agency (LLEA) was not properly marked, the release was not inappropriate because LLEAs are authorized access to SGI in accordance with 10 CFR 73.21.

OIG Response:

Whether or not LLEAs are authorized access to SGI does not mean they had an appropriate "need-to-know" and, therefore, does not negate that the release was inappropriate. The release was inappropriate as evidenced by the NRC official requiring that the document in question be returned to the agency and because is was not properly marked. Inappropriate releases of SGI are not simply determined on the merits of who received the information but also on whether they are properly handled and marked to ensure the information does not go to individuals other than intended.

Agency Comments:

Page 13, Section C, first paragraph (now page 8 of this report): Items 2 and 3 have nothing to do with a "Central Authority" needed for the oversight of the NRC SGI program. Secure telecommunication equipment acquisition and installation is covered under NRC's classified information program. It should also be noted that while NSIR controls the SGI program as a whole, it still relies on the expertise of the Office of the Chief Information Officer (OCIO) for equipment support, the Office of Administration for physical security oversight, and the Regions and program offices for oversight of licensees handling SGI.

Page 15 (now page 9 of this report): Although the equipment may be used to communicate SGI, the purchase of secure communications equipment for NRC resident offices was not done under the aegis of or to support the SGI program.

OIG Response:

The report identifies on page 9 that the secure telecommunications equipment was acquired and installed to ensure the agency could send classified information to the licensees. On page 11, OIG recognizes that an additional benefit of this equipment is using it to communicate SGI. Whether or not the equipment was directly acquired for use with classified information is not the point. Rather, in the context of this report and the agency's use of the equipment with SGI, issues related to the secure telecommunications equipment must be addressed by the agency to ensure it is available for use when needed.

Agency Comments:

In the section on Inadequate Training, NSIR has been coordinating training sessions that include the protection and handling of SGI since September 11, 2001. As of August 2003, approximately 90 percent of the agency has been trained on the proper handling requirements for SGI. NSIR has also issued agency announcements, created a cover sheet with handling and marking requirements on the reverse side, and created a new marking stamp that is consistent with current SGI requirements.

OIG Response:

OIG recognizes the coordinated training sessions in Section IV, "Management Initiatives," beginning on page 15 of the report. However, OIG's point is that training has been fragmented and, as implied in the agency response through NSIR's coordinating the training session, there is no single point of *ownership* for the training. Moreover, OIG's concern is that any actions taken to implement the recommendations in the report must be factored into any future training. As training in SGI is mandatory, any changes would have to be communicated during the required annual training. Moreover, in training the 10 percent of the agency staff who have not received instruction in the proper handling requirements for SGI, these factors should be considered.

Agency Comments:

Page 16, last paragraph (now page 11, second paragraph of this report): NSIR has always coordinated with OCIO for the installation of ISDN lines to operate secure telephone equipment and will continue to do so.

OIG Response:

OIG recognizes OCIO has been involved with coordinating the installation of ISDN lines. However, in context with the entire paragraph and the paragraph preceding it, OIG is identifying that coordination will have to take place among all responsible offices for future telecommunications equipment purchases to ensure the proper equipment is obtained, not just the installation of ISDN lines.

Agency Comments:

Page 18, Maintenance (now page 12 of this report): COMSEC Custodians are responsible for troubleshooting operational problems with secure equipment, rekeying secure telephones, and changing fuses associated with the equipment from time to time. With respect to maintenance, all equipment is required to be sent to a secure maintenance site when repairs are required.

OIG Response:

OIG clearly identifies that COMSEC Custodians are responsible for troubleshooting operational problems with secure equipment and is aware they are responsible for rekeying secure telephones. OIG disagrees that they are responsible for changing fuses associated with the equipment other than that located in headquarters and the regional offices. The inspectors or administrative assistants at the nuclear power plant sites perform that function when fuses need replacement. OIG recognizes and agrees that, except for replacing fuses and rekeying secure telephones, all equipment is required to be sent to a secure maintenance site when repairs are required.

Agency Comments:

In the section on Testing, it should be noted that the staff considers any use of secure telecommunication equipment to qualify as a test. Problems associated with secure telecommunication are frequently the result of operator error. In addition, many secure connections take several attempts to complete because of the multiplicity of settings possible for each phone and fax. This may even result from the differences in versions of equipment being used.

Page 19, second paragraph (now page 12, last paragraph of this report): Failure to be able to open a security container is usually due to operator error.

OIG Response:

OIG does not accept the premise that any use of secure telecommunications equipment qualifies as a test of that equipment. If the equipment fails when it is needed, it has failed in use, not during a test. Regular, periodic testing of the equipment would minimize the amount of human error associated with failures by building in familiarity with the equipment. Moreover, the agency will need to evaluate whether the differences in the versions of equipment being used is acceptable for the number of failures that have occurred. As to the failure of opening a security container due to operator error, this also can be minimized by regular, periodic testing which will require access to the contents of the security container.

Agency Comments:

Last paragraph (now page 13, first paragraph): Secure telecommunications equipment was primarily installed at Reactor Resident Inspector sites for transmission of classified information, not for SGI. If SGI needs to be sent outside a site on a non-emergency basis, it can be done thru U.S. Mail as has been practiced.

OIG Response:

See OIG's response to the agency's comments related to page 9.

Agency Comments:

Page 20, second paragraph (now page 13 of this report): NSIR has already taken the lead for coordinating and controlling the electronic transmission and processing program for SGI.

Last paragraph: OCIO has already rescinded NUREG/BR-0168, Rev. 2 entitled, "Policy for Processing and Handling Unclassified Safeguards Information and Other Sensitive Information in the NRC Local-Area/Wide-Area Network Environment," to eliminate the processing of SGI on the NRC LAN.

Page 21, (now page 13, last sentence of this report): The draft report states, "In short, SGI should not be processed on any computer that is or will be connected to the LAN." The report's corresponding Recommendation 6 ("Revise NRC procedures to eliminate the processing of SGI on the LAN") appears to be unnecessarily restrictive.

The draft report highlights an important fact, i.e., that existing guidance for automated processing of SGI is not consistent, and in some cases wrong. This may be addressed in other ways.

We recommend that Recommendation 6 be changed to read:

> "6. Revise documentation for NRC procedures to eliminate ~~the processing of SGI on the LAN~~ inconsistencies and ambiguities that could imply SGI can be processed on a

personal computer while it is connected to the unclassified NRC LAN, and to ensure that personal computers used for SGI processing while disconnected from the LAN do not employ fixed hard drives."

OIG Response:

OIG submitted its discussion and final draft reports to the agency in early September and late October 2003, as applicable, and the agency's response to the report was received December 12, 2003. In the interim, if agency staff have taken actions to address parts of the OIG recommended actions, they have not officially notified OIG nor provided any evidence of these actions. Moreover, OIG believes that recommendation 6 is appropriate as written.

Agency Comments:

Page 22, (now page 14 of this report): The report's Recommendations 4 and 5 deal with telecommunications equipment for transmitting SGI. Pages 16 through 19 of the report address acquisition, installation, maintenance, and testing of this equipment, detailing numerous problems with testing and reliability. On page 16, however, there is a statement about the availability of new equipment that can encrypt conversations through regular telephone lines, without the use of special equipment, such as STU-IIIs or STEs, or an ISDN line. The report appeared to encourage a switch to this new technology.

Recommendations 4 and 5 on page 22 seem to neglect this promising new and available technology, and focus instead on continuing to commit resources for the less reliable technology now owned by the NRC. They refer to a separate secure telecommunications network that may not be necessary if the new technology is used. Recommendations 4 and 5 should be revised to permit or encourage a switch to the new technology, rather than force NRC into spending large amounts of money to acquire, install, test, and maintain the current technology that involves supporting a separate secure telecommunications network.

The transition to a new secure telecommunications technology may not be instantaneous or painless, but the report's recommendations should not, in effect, restrict us to staying with the current technology longer than necessary. We suggest the following revisions to Recommendations 4 and 5:

"4. Provide adequate resources to ~~ensure the timely installation, maintenance, and troubleshooting of problems with~~ acquire, install, test, and maintain appropriate secure communications technology to effectively and efficiently support the secure telecommunications ~~equipment~~ needs of the NRC, as new technologies become available and affordable."

"5. Formalize a program for periodic testing and documentation of the currently installed secure telecommunications ~~network~~ systems to ensure continuing functionality for regular use and its readiness for emergency use."

<u>OIG Response:</u>

On page 11 of the report, OIG cited, as an example, that NSA officials said that new equipment is now available that can encrypt conversations through regular telephones. OIG did not corroborate this information or do any audit work to determine the feasibility of its use by NRC. As such, the agency would have to consider the application and cost of such equipment for future use by the agency. Until such time as the agency replaces the secure telecommunications equipment currently in place, NRC must ensure that the system it currently employs is properly installed, maintained, troubleshot, and tested. No revisions to the recommendations 4 and 5 are needed.