# U.S. NUCLEAR REGULATORY COMMISSION

# DIRECTIVE TRANSMITTAL

**TN**: DT-08-04

| | |
|---|---|
| To: | NRC Management Directives Custodians |
| Subject: | Transmittal of Management Directive 12.7, "NRC Safeguards Information Security Program" |
| Purpose: | Directive and Handbook 12.7 are being issued as a result of recommendations from the Sensitive Unclassified Non-Safeguards Information (SUNSI) Working Group that necessitated separating Safeguards Information (SGI) from the general definition for sensitive unclassified information. MD 12.7 specifically addresses SGI and includes changes in responsibilities, authorities, policies, and procedures for SGI. |
| Office and Division of Origin: | Office of Nuclear Security and Incident Response<br>Division of Security Operations |
| Contact: | Wayne Burnside, 301-415-2211 |
| Date Approved: | Approved: **June 25, 2008** |
| Volume: | 12 Security |
| Directive: | 12.7 NRC Safeguards Information Security Program |
| Availability: | Rulemaking, Directives, and Editing Branch<br>Office of Administration<br>Michael T. Lesar, 301-415-7163<br>Christy Moore, 301-415-7086 |

## OFFICE OF ADMINISTRATION

# NRC Safeguards Information Security Program

## Directive 12.7

# Contents

# NRC Safeguards Information Security Program Directive 12.7

## Policy
(12.7-01)

The policy of the U.S. Nuclear Regulatory Commission is to ensure that Safeguards Information (SGI) is properly handled and protected from unauthorized disclosure under pertinent laws, regulations, management directives (MDs), and applicable directives of other Federal agencies and organizations.

## Objectives
(12.7-02)

- Section 147 of the Atomic Energy Act of 1954, as amended, authorizes NRC to prescribe requirements for the regulation of SGI. (021)

- NRC intends to strike a balance between the public's right to information so they can meaningfully participate in the regulatory process and the need to protect sensitive security information from inadvertent release or unauthorized disclosure. (022)

- All NRC employees, contractors, and consultants who have access to documents containing SGI and activities involving this information must adhere to the authorities, responsibilities, and procedures specified in this directive and handbook. This directive and handbook do not affect Commission rules and regulations contained in the *Code of Federal Regulations* and

## Objectives
(12.7-02) (continued)

Orders that are applicable to NRC licensees and others (i.e., a certificate holder, vendors, and license applicants). This directive provides information security policy primarily associated with the preparation, handling, distribution, accountability, and protection of SGI, including that which is processed on information technology (IT) systems. The Federal Information Security Management Act (FISMA) as implemented by NRC through MD 12.5, "NRC Automated Information Security Program," specifies information protection requirements for information processed on NRC automated information systems. (023)

## Organizational Responsibilities and Delegations of Authority
(12.7-03)

### Commission
(031)

- Sets agency policy for SGI, including authorizing access to SGI by foreign nationals. (a)

- Authorizes distribution of SGI beyond what MD 12.7 already authorizes. (b)

### Executive Director for Operations (EDO)
(032)

Implements Commission policy for the NRC SGI Security Program, including the requirements for the protection of SGI for IT systems. Makes final determination on appeals of decisions that denied requests for information under the Freedom of Information Act (FOIA)/Privacy Act (PA) when any request involves information generated by offices reporting to the EDO.

## Organizational Responsibilities and Delegations of Authority
(12.7-03) (continued)

### Secretary of the Commission (SECY)
(033)

Makes a final determination on an appeal of an initial FOIA/PA decision in which SGI records were denied by the Executive Assistant to the Secretary of the Commission, the General Counsel, or any office director reporting to the Commission.

### Chief Information Officer (CIO)
(034)

- Develops and maintains an agencywide IT security program for SGI. (a)

- Assists senior agency officials with their IT security responsibilities for SGI. (b)

- Ensures that the agency has trained personnel sufficient to assist the agency in complying with IT security requirements for SGI. (c)

- Reports annually to the EDO and the Commission on the effectiveness of the agency IT security program for SGI, including progress of remedial actions. (d)

### Inspector General (IG)
(035)

Investigates instances of willful improper and unauthorized disclosures of SGI involving NRC employees, contractors, and consultants in violation of statutes and regulations. Makes a final determination on a FOIA/PA appeal of an initial decision of the Assistant Inspector General for Investigations (AIGI).

## Organizational Responsibilities and Delegations of Authority
(12.7-03) (continued)

### Deputy Executive Director for Reactor and Preparedness Programs (DEDR)
(036)

Directs and oversees the agency's SGI security programs.

### Computer Security Office (CSO)
(037)

- Administers NRC's IT security program. (a)
- Develops and maintains IT security policies, procedures, and control techniques for SGI to address all applicable requirements, including those issued under Section 3543 of FISMA and Section 11331 of Title 40. (b)
- Trains and oversees personnel with significant responsibilities for IT security for SGI. (c)
- Assists senior agency officials concerning their IT security responsibilities for SGI. (d)
- Ensures that the agency has trained personnel sufficient to assist the agency in complying with IT security requirements for SGI. (e)
- Reports annually to the CIO on the effectiveness of the agency IT security program for SGI, including progress of remedial actions. (f)
- Approves encryption for use in protecting SGI in systems and during transmission. (g)

## Organizational Responsibilities and Delegations of Authority
(12.7-03) (continued)

### Director, Office of Nuclear Security and Incident Response (NSIR)
(038)

Provides implementing guidance and direction for the NRC Information Security Program under which agency documents containing SGI are handled, consistent with the NSIR program. Ensures that the NRC SGI Security Program is carried out by the Division of Security Operations (DSO).

### Director, Office of Administration (ADM)
(039)

Provides implementing guidance and direction for the NRC personnel and physical security programs as they apply to SGI, consistent with the ADM program.

### Office Directors and Regional Administrators
(0310)

- Ensure that NRC employees, contractors, and consultant personnel under their jurisdiction are cognizant of and comply with the provisions of this directive and handbook. (a)

- Coordinate with DSO/NSIR and DFS/ADM on any existing or proposed SGI activities in organizations under their jurisdiction. (b)

- Report any significant change or termination of SGI activities to DFS for review of associated contracts, subcontracts, or similar actions. (c)

- Are responsible for conducting inquiries in instances of noncompliance with this directive and handbook and notify the

## Organizational Responsibilities and Delegations of Authority
(12.7-03) (continued)

### Office Directors and Regional Administrators
(0310) (continued)

EDO, DSO/NSIR, DFS/ADM, and OIG, as appropriate, in instances that may result in an infraction or a violation. (d)

- Request exceptions to or deviations from this directive and handbook, as required. (e)

### Director, Division of Security Operations (DSO), NSIR
(0311)

- Plans, develops, and administers policies, standards, and procedures for the NRC SGI Security Program, except the IT security program, consistent with the NSIR program. (a)

- Implements the NRC SGI Security Program within NRC. (b)

- Is responsible for the NRC SGI Security Program, including providing training for appropriate NRC personnel. (c)

### Director, Division of Facilities and Security (DFS), ADM
(0312)

- Monitors reports of noncompliance for SGI with applicable rules, regulations, and statutes; recommends corrective actions; and if necessary, conducts checks for persons other than NRC employees. When appropriate, reports this information to the Director of the Office of Administration, office directors, or regional administrators, consistent with the DFS program. (a)

## Organizational Responsibilities and Delegations of Authority
(12.7-03) (continued)

### Director, Division of Facilities and Security (DFS), ADM
(0312) (continued)

- Is responsible for approving SGI access for NRC contractors. (b)

- Establishes and ensures physical security requirements and protections for contractor facilities possessing SGI. (c)

## Applicability
(12.7-04)

This directive and handbook apply to all NRC employees and consultants and to all NRC contractors where compliance with this directive and handbook is a condition of a contract or a purchase order.

## Handbook
(12.7-05)

Handbook 12.7 provides security requirements for the preparation, distribution, accountability, and safeguarding of documents handled by NRC and its contractors that contain SGI.

## Exceptions or Deviations
(12.7-06)

Exceptions to or deviations from this directive and handbook may be granted by the Director of DSO except in those areas in which the responsibility or authority is vested solely with the Commission, the EDO, NSIR, CSO, or with DFS/ADM and is nondelegable; or for matters specifically required by law, Executive Order, or directive to be referred to other management officials. The protection procedures for SGI for individual IT

## Exceptions or Deviations
(12.7-06) (continued)

systems may deviate from the procedures for SGI in paper document form. Specific procedures for the protection of SGI in IT systems are contained in MD 12.5.

## References
(12.7-07)

*Code of Federal Regulations—*

10 CFR Part 2, "Rules of Practice for Domestic Licensing Proceedings and Issuance of Orders."

10 CFR Part 9, "Public Records."

10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities."

10 CFR Part 51, "Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions."

10 CFR Part 70, "Domestic Licensing of Special Nuclear Material."

10 CFR Part 71, "Packaging and Transportation of Radioactive Material."

10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

10 CFR 73.57, "Requirements for Criminal History Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees."

10 CFR 73.59, “Relief from Fingerprinting and Criminal History Records Check for Designated Categories of Individuals.”

10 CFR 73.71, "Reporting of Safeguards Events."

## References
(12.7-07) (continued)

10 CFR Part 1017, "Identification and Protection of Unclassified Controlled Nuclear Information" (Department of Energy, General Provisions).

U.S. Nuclear Regulatory Commission Documents

Management Directives

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

3.4, "Release of Information to the Public."

3.5, "Attendance at NRC Staff Sponsored Meetings."

5.5, "Public Affairs Program."

12.1, "NRC Facility Security Program."

12.2, "NRC Classified Information Security Program."

12.3, "NRC Personnel Security Program."

12.4, "NRC Telecommunications Systems Security Program."

12.5, "NRC Automated Information Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

NRC Orders

Relevant NRC Orders imposing additional security measures and NRC Orders imposing fingerprinting requirements for access to SGI and imposing measures for protection of SGI.

## References
(12.7-07) (continued)

NUREGs

NUREG-0794, "Protection of Unclassified Safeguards Information" (October 1981).

NUREG-0910, "NRC Comprehensive Records Disposition Schedule."

NUREG/BR-0069, Rev. 2, "NRC Classification Guide for National Security Information Concerning Nuclear Materials and Facilities" (CG-NMF-2) (December 1991).

NRC Designation Guide for Safeguards Information (DG-SGI-1).

*United States Code*

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

Energy Policy Act of 2005 (Pub. L. 109-58).

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

Federal Information Security Management Act of 2002.

Freedom of Information Act (5 U.S.C. 552).

Homeland Security Act of 2002 (6 U.S.C.A. 101 et seq.).

Inspector General Act (5 U.S.C. App. 3).

Privacy Act (5 U.S.C. 552a).

# NRC Safeguards Information Security Program

## Handbook 12.7

# Contents

## Part I



## Part II

# Contents (continued)



Exhibits

# Part I
# Introduction

## Purpose and Scope (A)

Requirements and procedures herein provide assurance that information containing Safeguards Information (SGI) is adequately protected from unauthorized disclosure. Specific procedures for the protection of SGI in information technology (IT) systems are contained in Management Directive (MD) 12.5, "NRC Automated Information Security Program." (1)

- SGI is defined as information the disclosure of which could reasonably be expected to have a significant adverse effect on the health and safety of the public 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. The unauthorized release of this information, for example, could result in harm to the public health and safety and the Nation's common defense and security or 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. (a)

- Further, SGi identifies a licensee's or applicant's detailed (1) security measures for the physical protection of special nuclear material, source material or byproduct material; (2) security measures for the physical protection and location of certain plant equipment vital to the safety of a facility possessing nuclear materials subject to NRC jurisdiction; (3) design features of the physical protection system; (4) operational procedures for the security organization; (5) improvements or upgrades to the security system; (6) consequences or weaknesses not yet corrected; and (7) such information as the Commission may designate by order. (b)

SGI-Modified Handling (SGI-M) is a special designation of SGI that specifically identifies a licensee's or an applicant's detailed security measures for the physical protection of byproduct material or source material. (2)

## Applicability (B)

NRC employees, consultants, and contractors are responsible for ensuring that the procedures specified in this part are followed to protect SGI pursuant to Section 147 of the Atomic Energy Act of 1954, as amended. The requirements of the MD will be imposed on pertinent contractors through the subject contract documents. (1)

The use of "contractor" in this part means any person, firm, unincorporated association, joint venture, co-sponsor, partnership, corporation, affiliate thereof, or their successors in interest, including their chief executives, directors, key personnel (identified in the contract), proposed consultants, or subcontractors that are party to a contract with NRC. (2)

## Authority for Controls (C)

The criteria for the control and handling of SGI are codified in Section 147 of the Atomic Energy Act of 1954, as amended, and 10 CFR 73.21.

## Authority To Designate SGI (D)

NRC employees, contractors, and consultants who have successfully completed the required SGI designation training and certification by the Information Security Branch, Division of Security Operations (DSO), NSIR, are authorized to make SGI determinations. Certification is evidenced by the successful completion of the SGI training modules. If a contract involves the processing of SGI, the contracting officer or authorized representative (project officer) has the authority to make SGI determinations. The project officer may designate specific contractor employees to make SGI determinations once they have successfully completed the required SGI determination training. (1)

Offices are required to have sufficient numbers of SGI designators trained and certified to make determinations. (2)

## Release of Information to the Public (E)

The presence or absence of SGI markings does not automatically determine whether a document may be withheld from the public. Each document requested by the public that may contain SGI must be reviewed against the NRC Designation Guide for SGI to determine whether the document actually contains SGI or not, and is releasable. (See MD 3.4, "Release of Information to the Public.") (1)

Whenever an NRC individual has a question regarding the releasability of information, the employee should consult with his or her supervisor or— (2)

- The Information and Records Services Division, Office of Information Services (OIS), if a request for information involves the Freedom of Information Act (FOIA), Sensitive Unclassified Non-Safeguards Information (SUNSI), the Privacy Act, or relates to the NRC's general public health and safety mission (see MDs 3.1, "Freedom of Information Act"; 3.2, "Privacy Act"; or 3.4, "Release of Information to the Public") (a)

- DSO/NSIR, on whether a document contains SGI (b)

- The Office of the General Counsel (OGC), or appropriate regional counsel, on legal questions (c)

## "No Comment Policy" for SGI (F)

Occasionally statements may appear in the public domain (e.g., newspaper and Internet) that contain SGI. The fact that the SGI appeared publicly does not make it decontrolled. It is NRC policy to neither confirm nor deny that information appearing in the public domain is or is not SGI. Any questions raised about the accuracy, sensitivity, or technical merit of such information should be responded to in a "no comment" manner. (1)

## "No Comment Policy" for SGI (F)
(continued)

For further details regarding the "no comment" policy, contact DSO. (2)

## SGI Official Agency Records (G)

SGI being retained for official agency recordkeeping may be stored in the SGI local-area network (LAN). SGI shall not be placed in the Agencywide Documents Access and Management System (ADAMS).

## SGI-Modified Handling (H)

Although information designated as SGI-M has modified handling requirements for licensees or applicants, it is NRC policy and practice that NRC employees and NRC contractors handle information designated as SGI-M in a manner identical to SGI.

# Part II
# Protection and Control of Safeguards Information

## Safeguards Information Originated by NRC and NRC Contractors (A)

**Access** (1)

A security clearance is not required for access to Safeguards Information (SGI). However, the employee, contractor, or consultant must possess an established "need-to-know." (a)

Before being given access to SGI, such individuals are subject to fingerprinting and a Federal Bureau of Investigation and criminal history records check unless they are exempt from such requirements. The following categories of individuals are exempt— (b)

- An employee of the Commission or of the Executive Branch of the United States Government who has undergone fingerprinting for a prior U.S. Government criminal history check (i)
- A member of Congress (ii)
- An employee of a member of Congress or congressional committee who has undergone fingerprinting for a prior U.S. Government criminal history check (iii)
- The Governor of a State or his or her designated State employee representative (iv)
- A representative of a foreign government organization that is involved in planning for, or responding to, nuclear or radiological emergencies or security incidents who the Commission approves for access to SGI (v)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Access** (1) (continued)

- Federal, State, or local law enforcement personnel (vi)

- State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives (vii)

- Agreement State employees conducting security inspections on behalf of the NRC pursuant to an agreement executed under Section 274.i. of the Atomic Energy Act of 1954, as amended (viii)

- Representatives of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who have been certified by the NRC (ix)

The individuals specified in the above list are normally considered to be trustworthy in view of their employment status and in accordance with NRC requirements. If there is any indication that the intended recipient would be unwilling or unable to provide the protection prescribed for SGI, access shall not be granted. The Commission may authorize additional distribution of SGI. (c)

When necessary to respond to a life-threatening emergency situation, SGI may be disclosed to others who are not otherwise eligible for access. (d)

**When Information Is Marked as SGI** (2)

Information in any form (e.g., electronic or hard copy) containing SGI must be marked accordingly.

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**How Information Is Marked** (3)

At the time it is determined that a document contains SGI, SGI designators must— (a)

- Mark each document to indicate the presence of SGI or SGI-M (Safeguards Information-modified handling) in a conspicuous manner on the top and bottom of each page. The first page of the document or other matter must also contain— (i)

  – the name, title, and organization of the individual authorized to make an SGI determination, and who has determined that the document or other matter contains SGI (*a*)

  – the date the determination was made (*b*)

  – a marking that unauthorized disclosure will be subject to civil and criminal sanctions (*c*)

- In addition to the markings at the top and bottom of each page, any transmittal letters or memoranda to or from the NRC that do not in themselves contain SGI shall be marked to indicate that attachments or enclosures contain SGI but that the transmittal document or other matter does not (i.e., “When separated from Safeguards Information enclosure(s), this document is decontrolled provided the transmittal document does not otherwise warrant protection from the unauthorized disclosure”). (ii)

- Any transmittal document or other matter forwarding SGI must alert the recipient that protected information is enclosed. Certification that a document or other matter contains SGI must include the name and title of the certifying official and date designated. (iii)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**How Information Is Marked** (3) (continued)

- Marking of documents or other matter containing or transmitting SGI shall, at a minimum include the words "Safeguards Information" to ensure identification of protected information for the protection of facilities and material covered by 10 CFR 73.22. (iv)

Multiple-page Documents (b)

The SGI or SGI-M markings must be placed at the top and bottom of—

- The outside of the front cover, if any (i)
- The title page, if any (ii)
- The first page of text, if there is no front cover or title page (iii)
- Each internal page of a document containing SGI (iv)
- Back cover (v)

Portion-Marking (c)

Portion-marking is accomplished by clearly indicating the portions (e.g., titles, paragraphs, subjects, or pages) that contain SGI by placing the abbreviation "SGI" or "SGI-M" in parentheses at the beginning or the end of the portion. If all portions of the document are SGI, a statement to that effect is sufficient without marking each paragraph. For example, the following marking may be used: "The entire document is SGI." (i)

Portion-marking is required when— (ii)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**How Information Is Marked** (3) (continued)

- A document contains several categories of sensitive unclassified information in order to distinguish SGI portions (e.g., paragraphs, pages, and appendices) from other portions containing other sensitive unclassified information (e.g., SUNSI [Sensitive Unclassified Non-Safeguards Information]). In such cases, SGI or SGI-M would be the overall marking used at the top and bottom of the page. (*a*)

- A document contains both classified information and SGI. Portion-marking indicates which portions contain each category. Portions (e.g., paragraphs) that contain both SGI and classified information must indicate which portions are classified and which portions are SGI. If a document is declassified and SGI remains, the document must be marked in accordance with the requirements stated in this part. If all portions of the text are SGI, a statement to this effect is sufficient without specifying or marking each item. (*b*)

- It is necessary to distinguish SGI portions from non-SGI. (*c*)

Files or Folders (d)

Files and folders containing SGI must be marked as SGI or SGI-M on the outside of the front and back covers upon creation or when extracted from an existing file system.

Other Media Containing SGI (e)

Other information media (e.g., computer disks, slides, film, etc.) containing SGI should be marked in accordance with the requirements set forth in this management directive (MD) to the extent possible.

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Cover Sheet** (4)

Each document containing SGI in the possession of NRC employees or NRC contractors must be covered by an SGI cover sheet (see Exhibit 1) to facilitate identification and protection of the information. Cover sheets are not required on documents that are inappropriately marked SGI files.

**Reproduction** (5)

Documents that contain SGI may be reproduced to meet operational requirements without permission of the originator or the office responsible for the document. Holders shall minimize the number of copies needed to conduct official business. Steps shall be taken to prevent unauthorized access during reproduction and in the disposition of matter containing SGI. Unneeded copies or improperly prepared copies shall be immediately destroyed. SGI may be reproduced on non-networked copiers accredited by the NRC's designated approving authorities (see MD 12.5, "NRC Automated Information Security Program"). All copies must clearly show the protective markings contained on the original document. (a)

Whenever the originator wants to limit the further dissemination or reproduction of documents containing SGI, the following statement shall be placed on the front of the document: "Reproduction or Further Dissemination Requires Approval of _____" (the name of the person who controls official reproduction). (b)

If reproduction services for SGI are requested, NRC Form 20, "Request for Printing and Copying Services," shall contain an explanation in the special instructions block that SGI is attached, and an asterisk shall be placed in the "Unclassified" and "Other" blocks. This action must be taken to ensure proper handling of the document and proper disposal of any waste (see Section (A)(12) of this part). The requester shall ensure that the markings on documents submitted for reproduction are in black or red and dark enough to be reproduced legibly. (c)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Non-Electronic Transmission** (6)

Documents containing SGI must be transmitted by one of the following methods:

- NRC interoffice mail in a single sealed opaque envelope within NRC Headquarters. (a)
- For transmission of SGI between NRC Headquarters and regional offices, NRC pouch mail with an inner envelope. (b)
- Outside NRC: In two opaque envelopes by U.S. Postal Service first class certified mail or by a delivery company that provides nationwide overnight service with computer tracing capability. (c)
- Hand-carried by any individual authorized access to SGI based on approval from the employee's division director or designee. (d)
- Outside the continental U.S.: By government-to-government mail channels or approved electronic means. (e)
- Other means approved by the Director of the Division of Facilities and Security (DFS), ADM. (f)

**Note**: Upon receipt and recognition of SGI, the recipient is expected to handle the document in accordance with normal procedures for the storage of SGI (e.g., appropriate handling and storage).

**Preparation for Transmission** (7)

**Note**: SGI must be under the control of a person who is authorized access or must be stored in either a GSA-approved security container or a file cabinet equipped with a locking bar equipped with GSA-approved padlock. The inner envelope or wrapper must have the words "Safeguards Information" at the top and bottom on

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Preparation for Transmission** (7) (continued)

both sides and be addressed to the intended recipient, with a return address included. (a)

When preparing documents containing SGI for transmission outside an NRC facility or an NRC contractor facility in accordance with the means identified in Section (A)(6) of this part, they must be enclosed in two opaque sealed envelopes or similar wrappings. The inner envelope or wrapper must show the name and address of the intended recipient and sender on the front and have the words "Safeguards Information" at the top and bottom on both sides. In addition, the inner envelope should be taped or sealed in such a manner that would indicate evidence of tampering. The outer envelope or wrapper must be addressed to the intended recipient, must contain the appropriate SGI address of the sender, and must not bear any markings or indication that the document contains SGI. (b)

**Electronic Transmission** (8)

All routine electronic transmissions of SGI must be protected by appropriately accredited means. Minimal requirements for such equipment and cryptography are specified by the National Institute of Standards and Technology in Federal Information Processing Standard (FIPS) 140-2. Such equipment is commercially available and may be in the form of telephones, software encryption for e-mail transmission, or other products. Information on implementation protocols, key management, key exchange, or other protection issues for SGI are available in MD 12.5. (a)

Approval for the use of specific hardware or software security procedures implementing transmission protection of SGI resides with CSO as described in MD 12.5. The requirement for security plans and other documentation for the certification/accreditation and use of these protective measures should be coordinated with CSO as described in MD 12.5. (b)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Electronic Transmission** (8) (continued)

Emergency communication of SGI that may have some bearing on catastrophic events or loss of life should be communicated by the most expeditious means and then reported to the Chief of the Information Security Branch (ISB), Division of Security Operations (DSO), NSIR, and to the Director of DFS, ADM. (c)

SGI may not be processed into the Agencywide Documents Access and Management System (ADAMS). (d)

In accordance with MD 12.5, an authority to operate is required before SGI is electronically transmitted. (e)

**Information Technology Processing** (9)

SGI must be processed on a standalone personal computer (PC), a PC physically disconnected from the LAN (local area network) with a removable hard drive, or over an accredited network (e.g., FIPS 140-2). Refer to MD 12.5.

**Protection During Use** (10)

Documents containing SGI must be under the control of an individual authorized access. The documents must not be left unattended, except as authorized in a limited access area approved by DFS. SGI shall be protected to avoid disclosing the information to unauthorized persons.

**Storage** (11)

SGI must be stored in a locked security storage container when unattended or not in actual use. (a)

As the term is used in this part, "security storage container" includes any of the following containers: (b)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Storage** (11) (continued)

- A steel filing cabinet equipped with a steel locking bar and a three-position changeable combination, GSA-approved padlock for storage in NRC Headquarters and regional office buildings with sufficient controls to prevent unrestricted access to the container. An NRC office that is occupied by employees during working hours and locked during nonworking hours (cleaning personnel may have keys, if necessary) would be considered to have sufficient access controls. This steel filing cabinet would not be considered adequate for a general public area (e.g., a Public Document Room). (i)

- A security filing cabinet that bears a test certification label on the side of the locking drawer, or on an interior plate, and that is marked as a "General Services Administration Approved Security Container." (ii)

- A bank safe deposit box. (iii)

- Other containers approved in writing by the Director of DFS. (iv)

The lock combinations protecting SGI must be limited to a minimum number of persons who have a "need-to-know" to conduct official business and are otherwise authorized access to them in accordance with the provisions of this MD. Combinations must be changed when placed in use, whenever a person having access no longer has an official need-to-know, when a person has access terminated, or when the combination is compromised. (c)

Security storage containers to be removed for repair or maintenance, returned to the supplier, or otherwise taken out of service for any reason must be examined to ensure that no SGI documents remain therein. (d)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Destruction of SGI** (12)

Holders of SGI documents are responsible for destroying these documents when they are no longer required. (a)

SGI must be destroyed using methods of destruction that preclude reconstruction (i.e., shredding or burning). SGI may also be placed in classified waste receptacles located throughout NRC buildings. Electronic media/equipment containing classified information or SGI are to be destroyed as described in MD 12.5 or sent to DFS/ADM for destruction. (b)

Destruction records for SGI are not required. (c)

**Residential Use** (13)

Employees are prohibited from using, handling, or storing SGI at their residences except as authorized in NRC's SGI Travel Procedures (see Exhibit 2).

**Telecommuting Policy** (14)

Residential use, handling, or storage of SGI for the purpose of telecommuting is prohibited.

**Use of SGI During Official Travel** (15)

Use of SGI during official travel by NRC employees is not generally authorized since other means of advance transmission (i.e., mail and secure facsimile) are usually available except as authorized in NRC's SGI Travel Procedures (see Exhibit 2). (a)

Handling and storage of SGI during official NRC travel are only authorized to conduct official business when other means of advance transmission and secure storage are not available or feasible as approved in writing by the employee's division director or designee. DFS shall be provided a copy. (b)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Use of SGI During Official Travel** (15) (continued)

Procedures for NRC employees or contractors handling SGI while on official travel are described in Exhibit 2. (c)

**Removal of Information From the SGI Category** (16)

Necessity for Review (a)

The systematic review of documents or files containing SGI to determine whether these documents should remain in this category is not required. However, it is NRC policy to decontrol all protected information at the earliest practicable date. This review is necessary only when specific circumstances require such action. For example, transportation schedules for spent fuel shipments are decontrolled 2 days after the shipment arrives at its ultimate destination, provided that release of such information does not reveal information that could be exploited by an adversary to affect operations of a facility or cause a radiological release. Typically, a request for the information under the Freedom of Information Act or the Privacy Act would necessitate a review of this type. (i)

If the originator of a document containing SGI knows in advance that the information can be decontrolled on a certain date or event, he or she can denote the decontrol marking on the designation block. (ii)

Who May Remove Information From the SGI Category (b)

Any individual authorized to determine that a document contains SGI may remove the marking or indicate that it may be removed whenever the information no longer meets the requirement for protection as SGI (under appropriate MDs, guides, or regulations), provided the following individuals are informed: (i)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Removal of Information From the SGI Category** (16) (continued)

- The individual who originally determined that the document contained SGI or his or her successor (*a*)

- A supervisor of either of the above individuals (section chief or higher level official) or other individual identified in writing by the appropriate office director (*b*)

If there is a disagreement over a change of categories, the procedure set forth in Section (A)(16)(d) of this part must be followed. (ii)

Marking (c)

When Information Is Marked (i)

The following is the required marking to indicate that a document has been removed from the SGI category.

Removed from SGI category (on) or (after) (date or event)

| _____ | _____ | _____ | _____ |
|---|---|---|---|
| (Signature of person making determination) | (Title) | (Office) | (Date) |

This marking shall appear in a prominent location on the document.

Change in Category (ii)

Documents must be marked to indicate a change in category, the person who is responsible for the change, and the date of the change. For example, if the document is removed from the SGI

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Removal of Information From the SGI Category** (16) (continued)

category but will still contain 10 CFR 2.390 information or other sensitive unclassified information, the SGI markings must be removed and the document marked accordingly.

Removal of Markings (iii)

At a minimum, the SGI markings on the first page of text and on the outside of the front and back covers, if any, must be blacked out upon removal of a document from the SGI category or upon a change in the category. In the latter case, the new category must be inserted. If there are no covers, the marking must be blacked out or changed on the title page. If there is no title page, the marking must be blacked out or changed on the first page of text and on the outside of the back page. (*a*)

Persons possessing copies of the document who are advised that the markings are no longer required or that the markings must be changed shall use a marker to black out or change the SGI markings on the copies in their possession and indicate on each copy the authority for deleting or changing the markings. (*b*)

Exception: Large file rooms and copy distribution centers possessing multiple copies are not required to black out or change the markings but must maintain the notification that directs the removal or change to markings as a record of the action taken. At such times as copies are transmitted outside these rooms or centers, they must be appropriately marked to indicate their content. If the documents are not removed from the room, no change is required. (*c*)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**Removal of Information From the SGI Category** (16) (continued)

Disagreement on Changes of Category (d)

All differing opinions as to whether a document should be removed from the SGI category must be referred to the Director of DSO, NSIR, for final determination. Other disagreements regarding the removal of SGI from a category or a change in category regarding the matter should be referred to the office that generated the information.

**Inadvertent or Unauthorized Release of SGI** (17)

In accordance with MD 3.4, "Release of Information to the Public," the responsible office director must promptly inform the Executive Director for Operations, DSO, DFS, and the Inspector General in writing whenever SGI is inadvertently released or disclosed by NRC or its contractors. Inadvertent disclosure consists of providing information to anyone who does not possess the required access and need-to-know. Refer to MD 12.5 for any electronic release of SGI. (a)

The Office of the Inspector General (OIG) will be notified immediately by telephone when an unauthorized disclosure occurs with a written followup within 24 hours of the release or disclosure of SGI to the public. (b)

**NRC Contractor Security Requirements** (18)

NRC offices and divisions must promptly notify DFS of their intent to initiate a contract involving access to or possession of SGI. A completed NRC Form 187, “Contract Security and/or Classification Requirements,” and a statement of work must be submitted to DFS and a copy provided to DSO. Work on any contract (or purchase order) involving SGI cannot commence before approval by DFS. (a)

## Safeguards Information Originated by NRC and NRC Contractors (A) (continued)

**NRC Contractor Security Requirements** (18) (continued)

Contractors desiring onsite possession of SGI are subject to security inspections to determine eligibility to store and handle SGI. Contractor Statements of Work involving SGI are submitted by the Division of Contracts to the Director of DFS and a copy provided to DSO in accordance with MD 11.1, "NRC Acquisition of Supplies and Services." Work on any contract or purchase order involving SGI cannot commence prior to written approval by the Director of DFS. Refer to MD 12.5 for IT requirements for SGI. (b)

## NRC Designation Guide for SGI (B)

An NRC Designation Guide for SGI is available on the NRC internal Web site under the security topic, or in hard copy from NSIR/DSO/ISB.

**Approval of the NRC Designation Guide for SGI** (1)

The Director of DSO shall approve the NRC Designation Guide for SGI.

**Review of the NRC Designation Guide for SGI** (2)

The NRC Designation Guide for SGI shall be reviewed for currency every 5 years.

**Dissemination of the NRC Designation Guide for SGI** (3)

The NRC Designation Guide for SGI shall be distributed as widely as necessary to ensure proper awareness.

## SGI Originated by Sources Other Than NRC, NRC Contractors, and NRC Licensees (C)

**General Rule**

SGI originated by any person (whether or not an NRC employee, contractor, licensee, including Agreement State licensee, or license applicant and permit and certificate holders) must be protected and disseminated under the same security measures set forth in Section (A) of this part.

## Hearings, Conferences, or Discussions (D)

**Security Preparations Required for Hearings, Conferences, or Discussions** (1)

NRC employees, consultants, and contractor personnel who arrange or participate in hearings, conferences, or discussions (see MD 3.5, "Attendance at NRC Staff Sponsored Meetings") involving SGI shall—

- Ensure before a hearing, conference, or discussion that participating personnel are identified and are authorized to have access to the information to be discussed (a)
- Indicate to participating personnel that the specific information they will receive is SGI and advise them of the protective measures required (b)
- Ensure that no discussion takes place that is audible or visible to persons not authorized access to the information (c)
- Ensure that cellular telephones are not permitted in the meeting room. (d)

## Hearings, Conferences, or Discussions (D) (continued)

**Locations** (2)

Conferences involving SGI should be held within NRC guarded or controlled areas, if practical, with the exception of inspection exit interviews held at locations owned and controlled by NRC licensees. NRC division directors and above are authorized to establish conferences involving SGI. Conferences may be held outside guarded or controlled areas only when DFS is consulted for the purposes of obtaining appropriate guidance for the physical protection of SGI.

# Exhibit 1
# Safeguards Information Cover Sheet and Document Marking

NRC FORM 461
(MM-YYYY)

U.S. NUCLEAR REGULATORY COMMISSION

**SAFEGUARDS INFORMATION**

THIS DOCUMENT CONTAINS INFORMATION WHICH MUST BE PROTECTED FROM UNAUTHORIZED DISCLOSURE IN ACCORDANCE WITH THE FOLLOWING STATUTES AND NRC REGULATIONS THAT APPLY:

NRC MANAGEMENT DIRECTIVE 12.7
10 CFR 73.21
SECTION 147, ATOMIC ENERGY ACT OF 1954, AS AMENDED.
SECTION 149, ATOMIC ENERGY ACT OF 1991, AS AMENDED.

VIOLATIONS ARE SUBJECT TO CIVIL OR CRIMINAL PENALTIES.

THIS DOCUMENT IS NOT TO BE LEFT UNATTENDED OR ACCESSIBLE TO UNAUTHORIZED PERSONS. WHEN NOT IN USE, IT MUST BE STORED IN A LOCKED SECURITY STORAGE CONTAINER.

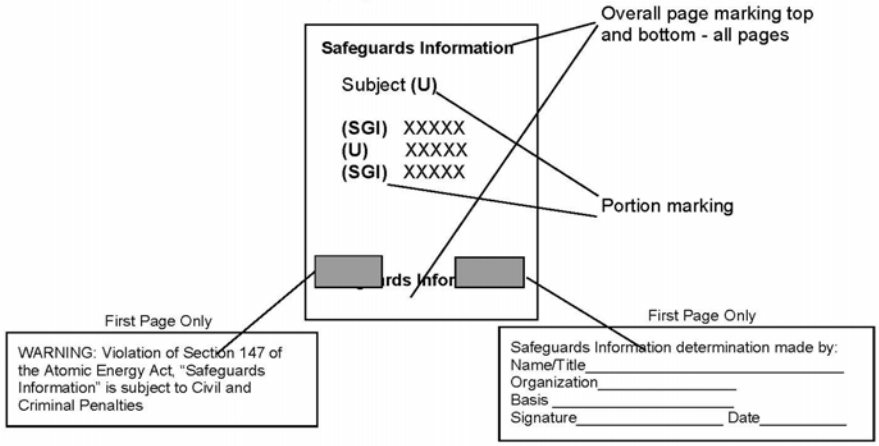
IT IS YOUR RESPONSIBILITY TO PROTECT THE INFORMATION CONTAINED IN THIS DOCUMENT FROM COMPROMISE, THEFT, OR UNAUTHORIZED DISCLOSURE.

**SAFEGUARDS INFORMATION**

# Exhibit 1 (continued)

**NRC REQUIRED MARKINGS:**

**SAFEGUARDS INFORMATION (SGI)**




| | |
|---|---|
| ACCESS: | Meets the requirements of 10 CFR 73.21 (c), NRC Management Directive 12.7, or other NRC requirements, **and** has a need-to-know. |
| STORAGE: | In an approved, locked security container when not in use. See Management Directive 12.7, Part II, "Protection and Control of SGI," or alternative NRC guidance for more information on approved containers. |
| MAIL: | USPS first class, certified, or overnight mail, or a commercial carrier with an electronic tracking system. |
| WRAPPING: | Use two opaque envelopes, mark inner envelope "Safeguards Information," the address, return address, and the intended recipient. On outer envelope use address and return address. **Do not** indicate the level of information contained on the outer envelope. |
| ELECTRONIC TRANSMISSION: | Secure telephone, Secure Facsimile or other NRC approved method, e.g., a system that is compliant with Federal Information Processing Standard (FIPS)140-2. |
| IT PROCESSING: | Process **only** on a standalone PC, a PC physically disconnected from the LAN with a removable hard drive (Note: the application software and data must reside on the removable hard drive), or over an approved network (e.g., FIPS 140-2 compliant). |
| ADAMS: | **Do not** enter documents containing Safeguards Information into ADAMS. (Letters or memos used to transmit SGI may go into ADAMS without the SGI enclosure **if they do not contain SGI themselves**). |

# Exhibit 2
# Safeguards Information Travel Procedures

**General Policy**

Use of Safeguards Information (SGI) during official travel for NRC employees and contractors is not generally authorized because other means of advance transmission (i.e., mail or secure facsimile) and secure storage are usually available. However, when determined that advance means of transmission and storage are not available or feasible as approved by an employee's division director, if authorized to make SGI determinations, the following procedures apply: (**Note**: DFS shall be informed of instances in which SGI is handled or stored by employees during official travel.)

a. Pre-departure

- Written approval must be obtained in advance from a division director or his or her designee to possess and use SGI during official travel. DFS shall also be notified in advance.

- Specifics regarding the approval must include the name of the traveler, a nonsensitive description of the SGI, authorized work locations, approval date, and a statement that alternative methods of transport are neither feasible or available.

- The approval itself should not contain SGI. It is not required that the approval be carried while on travel. The approval should remain on file, with a copy to the information security staff, until the need to hand-carry SGI on official travel is terminated.

- SGI must be double-wrapped in two envelopes. The inner envelope must be tamper-indicating and marked as SGI at the top and bottom and front and back. The inner envelope must also contain a return address. The outer envelope must also be tamper-indicating, but it should not be marked in any way to indicate the presence of SGI. Note: Use of a lockable secure storage pouch may serve as an envelope.

b. In-use while on travel

- In the event that conditions make it impossible to store SGI at the work location (e.g., in approved storage containers authorized for use by resident inspectors), the traveler must exercise discretion to determine the best method for providing the

## Exhibit 2 (continued)

highest assurance that the information is not identified as SGI by casual observation and will be protected against unauthorized disclosure. Choices for temporary storage may include a hotel safe or a safety deposit box. However, SGI that is properly wrapped may be stored for periods not to exceed 12 hours per storage period. DFS should be consulted/informed for guidance.

- If none of these options are available, the traveler must retain positive control of the information at all times.

- Properly wrapped SGI may be taken to an employee's home before or after official travel for a 24-hour period if it is outside official duty hours.

c. Computer processing of SGI while on travel

- SGI must only be processed on an accredited laptop computer devoted strictly to SGI or equipped with a removable hard drive in accordance with an accredited computer security plan (see Management Directive 12.5, "NRC Automated Information Security Program").

- If the laptop computer is not equipped with a removable hard drive, the entire computer must be physically treated as SGI, including placing it in tamper-indicating packaging.

- If the laptop is equipped with a removable hard drive, it must be configured to "boot up" from the operating system on the removable drive.

d. Reproduction of SGI

SGI must be reproduced in accordance with established CSO procedures.

e. Procedures for handling SGI at airports

In the event that SGI is subject to security checks by airport security/U.S. Customs personnel, it is the traveler's responsibility to make the following efforts to prevent SGI from being opened by airport security/U.S. Customs personnel:

## Exhibit 2 (continued)

- The traveler must carry and be prepared to produce an "Authority to Hand-Carry" letter on NRC letterhead signed by the traveler's division director or higher level authority that describes the general nature of the information and explains why the SGI package must not be opened.

- The letter that identifies the person responsible for hand-carrying the document should be produced only if airport security/U.S. Customs personnel insist on opening the SGI package.

- If, upon producing the letter, airport security personnel still insist on opening the SGI package, the traveler should not intervene further.

f. Reporting

During official travel, if a traveler determines that SGI has been lost or potentially compromised, including checks by security airport personnel, the traveler must promptly notify the approving official who shall then promptly notify the Director of the Division of Facilities and Security and the Director of the Division of Security Operations (DSO). Such incidents must be reported to all appropriate offices, including OIG, within 24 hours of discovery of the fact that SGI may have been lost or potentially compromised. Upon return from official travel, any problems should be reported to the Information Security Branch, DSO, NSIR, for trending analysis. In the event of electronic loss of SGI, refer to MD 12.5.