U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 12.7 NRC SAFEGUARDS INFORMATION SECURITY PROGRAM DT-17-229

Volume 12	Security
Approved by:	Mark A. Satorius Executive Director for Operations
Date Approved:	June 27, 2014
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.
Issuing Office:	Office of Nuclear Security and Incident Response Division of Security Operations

Contact Name:	Robert Norman 301-415-2278	Krista Ziebell 301-415-7121

EXECUTIVE SUMMARY

Directive and Handbook 12.7 are being updated to reflect changes in the organizational responsibilities, structure, and processes that support the U.S. Nuclear Regulatory Commission Safeguards Information (SGI) Security Program; recommendations from the Office of the Inspector General; and Federal information security laws, mandates, and leading best practices. This revision incorporates NRC policy changes that are related to information security handling requirements, including—

- Clarification of how non-SGI information may become SGI in the aggregate;
- Clarification on NRC expectations regarding social media and SGI;
- Recommendations from the requirements in COMSECY-04-0034, "Additional Steps to Regularize Clearances for Classified Information Exchanges with NRC's Primary Partner Countries," dated June 14, 2004;
- Guidance from the Staff Requirements Memorandum on SECY-14-0014, "Sharing of Safeguards Information with the International Atomic Energy Agency and other Multilateral Organizations," dated May 7, 2014; and
- Changes to Title 10 of the *Code of Federal Regulations*, Part 73, Section 22, that have been instituted since the previous publication of Management Directive 12.7 in 2008.

This revision also incorporates recommended changes resulting from the Office of the Inspector General Audit, OIG-12-A-12, "Protection of Safeguards Information," dated April 16, 2012, including the new reporting structure for one point of contact to report SGI release, the responsibility for the SGI release tracking system, and guidance on granting "outsiders" access to SGI and the incorporation of interim policy on the day-to-day safekeeping and storage of SGI.

TABLE OF CONTENTS

I. POLICY....2

II. OBJECTIVES....3

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY....3

A. Commission....3
B. Executive Director for Operations (EDO)....3
C. Secretary of the Commission (SECY)....4
D. Deputy Executive Director for Reactor and Preparedness Programs (DEDR)....4
E. Deputy Executive Director for Corporate Management (DEDCM)....4
F. Inspector General (IG)....4
G. Director, Office of International Programs (OIP)....4
H. Director, Office of Nuclear Security and Incident Response (NSIR)....5
I. Director, Computer Security Office (CSO)....5
J. Director, Office of Administration (ADM)....5
K. Chief Human Capital Officer (CHCO)....5
L. Office Directors and Regional Administrators....6
M. Director, Division of Security Operations (DSO), NSIR....6
N. Director, Division of Facilities and Security (DFS), ADM....6

IV. APPLICABILITY....7

V. DIRECTIVE HANDBOOK....7

VI. EXCEPTIONS OR DEVIATIONS....7

VII. PROTECTION OF SAFEGUARDS INFORMATION IN NRC INFORMATION TECHNOLOGY SYSTEMS....7

VIII. REFERENCES....8

I. POLICY

It is the policy of the U.S. Nuclear Regulatory Commission to ensure that Safeguards Information (SGI) is properly handled and protected from unauthorized disclosure in accordance with the Atomic Energy Act (AEA) of 1954, as amended (42 U.S.C. 2011 et seq.); Management Directive (MD) 12.1, “NRC Facility Security Program”; MD 12.5, “NRC Cyber

Security Program"; and applicable laws and directives of other Federal agencies and organizations.

II. OBJECTIVES

- Section 147 of the AEA of 1954, as amended, authorizes NRC to prescribe requirements for the regulation of SGI.
- 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.
- 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 MD.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Commission

1. Sets agency policy governing SGI, including authorizing access to SGI by foreign nationals.
2. Authorizes distribution of SGI beyond what MD 12.7 already authorizes.

B. Executive Director for Operations (EDO)

1. Implements Commission policy for the NRC SGI Security Program, including the requirements for the protection of SGI for Information Technology (IT) systems.
2. Delegates to the Deputy Executive Director for Corporate Management (DEDCM) the authority to make a final determination on an appeal of an initial denial of a Freedom of Information Act (FOIA) (5 U.S.C. 552) request or a denial under the Privacy Act (PA) (5 U.S.C. 552a) by an office reporting to the Executive Director for Operations (EDO).
3. Makes the final determination on an appeal of a denial for a waiver or a reduction of fees, or a denial of a request for expedited processing.
4. Approves in writing, or delegates the authority to approve, the handling and storage of SGI during official travel and provides a copy of that approval to the Director of the Office of Administration (ADM).

C. Secretary of the Commission (SECY)

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.

D. Deputy Executive Director for Reactor and Preparedness Programs (DEDR)

1. Directs and oversees the agency's SGI security programs.
2. Delegates authority to the Director of the Office of Nuclear Security and Incident Response (NSIR) to manage the NRC Information Security Program.

E. Deputy Executive Director for Corporate Management (DEDCM)

1. Serves as the agency Chief Information Officer, Chief Freedom of Information Act Officer, and Senior Accountable Official for Data Quality.
2. As delegated by the EDO, makes a final determination on an appeal of an initial denial of a FOIA request or a denial under the PA by an office reporting to the EDO.
3. Develops and maintains an agencywide IT security program for SGI.
4. Assists senior agency officials with their IT security responsibilities for SGI.
5. Ensures that the agency has trained personnel sufficient to assist the agency in complying with IT security requirements for SGI.

F. Inspector General (IG)

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

G. Director, Office of International Programs (OIP)

1. Administers agency-to-agency international agreements for the sharing of sensitive information, including SGI.
2. Makes a net advantage determination for the NRC when a foreign Government or entity requests access to sensitive information. Also coordinates the need-to-know request with applicable program offices after a net advantage determination has been made in accordance with the agreed-upon procedural guidelines coordinated between NSIR and OIP, issued on February 2, 2011.

3. Serves as the NRC point of contact for taking receipt of and coordinating requests for SGI from an international agency, foreign entity, or multilateral organization.
4. Requests permission from the Commission for the release of SGI, and obtains the non-disclosure assurance of the international entity or organization. Notifies the Commission of additional SGI requests made by that entity via a Commissioner Assistant Note.
5. Maintains cognizance over all international agreements, and maintains a record of agency-to-agency international agreements. These agreements contain specific references for distributing documents received under these agreements.
6. Consults with NSIR regarding the protection of and dissemination of SGI.

H. Director, Office of Nuclear Security and Incident Response (NSIR)

1. Provides implementing guidance and direction for the NRC SGI Security Program.
2. Establishes and monitors the agency's security requirements for the handling of the agency's documents containing SGI, consistent with NRC requirements.
3. Delegates authority to the Division of Security Operations (DSO), NSIR, to manage the NRC SGI Security Program.

I. Director, Computer Security Office (CSO)

1. Plans, directs, and oversees the implementation of the agencywide Cyber Security Program, to include the electronic processing of SGI.
2. Responds to cyber security incidents, to include proper and timely reporting to the United States Computer Emergency Readiness Team (US-CERT).
3. Keeps the NRC apprised of current cyber security threats, vulnerabilities, and mitigation measures.

J. Director, Office of Administration (ADM)

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

K. Chief Human Capital Officer (CHCO)

1. Coordinates with NSIR to prepare and revise training and training material as required.

2. Coordinates with the Senior Program Manager for Safeguards Information, DSO, NSIR, for the creation and revision, when necessary, of the Safeguards Information Designation Official certification training material.

3. Notifies NRC employees, contractors, and consultants when refresher training is required for those personnel identified as Safeguards Information Designators.

L. Office Directors and Regional Administrators

1. Ensure that NRC employees, contractors, and consultant personnel under their jurisdiction are cognizant of and comply with the provisions of this MD.

2. As the responsible office, ensure that sharing SGI with an outsider will be conducted in accordance with the provisions of this MD.

3. Coordinate with the Director of DSO, NSIR, and the Director of the Division of Facilities and Security (DFS), ADM, on any existing or proposed contracts or contract activities that may require access to SGI in organizations under their jurisdiction.

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

5. Responsible for conducting inquiries in instances of noncompliance with this MD and notifying the EDO; DSO, NSIR; DFS, ADM; and OIG, as appropriate, in instances that may result in an incident or a violation.

6. Request exceptions to or deviations from this MD, as required.

M. Director, Division of Security Operations (DSO), NSIR

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

2. Implements the NRC SGI Security Program within NRC.

3. Ensures SGI training is provided for appropriate NRC personnel.

N. Director, Division of Facilities and Security (DFS), ADM

1. Reviews and monitors reports of noncompliance for SGI with applicable rules, regulations, and statutes; recommends corrective actions; and if necessary, conducts background checks for persons other than NRC employees. When appropriate, reports this information to the Director of ADM, office directors, or regional administrators, consistent with the ADM program.

2. Serves as the agency's central contact for reporting non-compliance with SGI handling, processing, and storage requirements. Tracks, monitors, and analyzes SGI-related trends.
3. Approves SGI access for NRC contractors.
4. Establishes and ensures physical security requirements for contractor facilities possessing SGI.

IV. APPLICABILITY

A. This MD applies 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.

B. This MD does not affect Commission rules and regulations contained in the *Code of Federal Regulations* and NRC orders that are applicable to NRC licensees and others (i.e., a certificate holder, vendors, and license applicants).

V. DIRECTIVE HANDBOOK

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

VI. EXCEPTIONS OR DEVIATIONS

Exceptions to or deviations from this directive and handbook may be granted by the Director of DSO, NSIR, 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 systems may deviate from the procedures for SGI in paper document form.

VII. PROTECTION OF SAFEGUARDS INFORMATION IN NRC INFORMATION TECHNOLOGY SYSTEMS

This directive provides the information security policy primarily associated with the preparation, handling, distribution, accountability, and protection of SGI. MD 12.5, "NRC Cyber Security Program," provides the policy for electronic processing of SGI.

VIII. REFERENCES

Code of Federal Regulations

10 CFR Part 2, "Agency Rules of Practice and Procedure."

10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding."

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 Part 73, "Physical Protection of Plants and Materials."

10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements."

10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements."

10 CFR 73.23, "Protection of Safeguards Information-Modified Handling: Specific Requirements."

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

10 CFR 73.59, "Relief from Fingerprinting and Criminal History Records Checks and Other Elements of Background Checks for Designated Categories of Individuals."

10 CFR 73.71, "Reporting of Safeguards Events."

10 CFR Part 1017, "Identification and Protection of Unclassified Controlled Nuclear Information."

Department of Energy (DOE) Order 471.6, "Information Security," June 20, 2011.

Nuclear Regulatory Commission

Computer Security Office Standard (CSO-STD) 2004, "Electronic Media and Device Handling Standard," available at http://www.internal.nrc.gov/CSO/standards.html (ML100210148).

COMSECY-04-0034, “Additional Steps to Regularize Clearances for Classified Information Exchanges with NRC’s Primary Partner Countries,” June 14, 2004.

Interim Guidance on the Use of Social Media, dated December 28, 2010 (ML103060402).

Management Directive—

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.”

11.1, “NRC Acquisition of Supplies and Services.”

12.1, “NRC Facility Security Program.”

12.3, “NRC Personnel Security Program.”

12.5, “NRC Cyber Security Program.”

12.6, “NRC Sensitive Unclassified Information Security Program.”

Memorandum from James T. Wiggins in response to Staff Requirements Memoranda (SRM) related to COMSECY-04-0006 (February 19, 2004) and COMSECY-10-0006 (July 28, 2010), “Sharing Classified and Safeguards Information” (also known as procedural guidance for NSIR and OIP), dated February 2, 2011 (ML110280034).

NRC DG-SGI-1, “NRC Designation Guide for Safeguards Information,” available at http://nsir.nrc.gov/pdf/Designation%20Guide%20for%20Safeguards%20Information.pdf.

NRC Forms Library on SharePoint: http://fusion.nrc.gov/nrcformsportal/default.aspx.

NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information, available at http://www.internal.nrc.gov/sunsi/pdf/SUNSI-Policy-Procedures.pdf.

NRC Security Web site: http://www.internal.nrc.gov/security.html.

NUREG-0910, “NRC Comprehensive Records Disposition,” March 2005.

OIG-12-A-12, “Audit of NRC’s Protection of Safeguards Information,” dated April 16, 2012 (ML12107A048).

SRM on SECY-14-0014, “Sharing of Safeguards Information with the International Atomic Energy Agency and Other Multilateral Organizations,” May 7, 2014 (ML14127A587).

Yellow Announcement YA-05-0077, “Policy Revision: NRC Policy and Procedures for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information (SUNSI),” October 26, 2005 (ML051220278).

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 (Pub. L. 107-347, Title III).

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

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

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

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

DH 12.7 NRC SAFEGUARDS INFORMATION SECURITY PROGRAM DT-17-229

Volume 12:	Security	
Approved by:	Mark A. Satorius Executive Director for Operations	
Date Approved:	June 27, 2014	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of Nuclear Security and Incident Response Division of Security Operations	
Contact Name:	Robert Norman 301-415-2278	Krista Ziebell 301-415-7121

EXECUTIVE SUMMARY

Directive and Handbook 12.7 are being updated to reflect changes in the organizational responsibilities, structure, and processes that support the U.S. Nuclear Regulatory Commission (NRC) Safeguards Information (SGI) Security Program; recommendations from the Office of the Inspector General; and Federal information security laws, mandates, and leading best practices. This revision incorporates NRC policy changes that are related to information security handling requirements, including—

- Clarification of how non-SGI information may become SGI in the aggregate;
- Clarification on NRC expectations regarding social media and SGI;
- Recommendations from the requirements in COMSECY-04-0034, "Additional Steps to Regularize Clearances for Classified Information Exchanges with NRC's Primary Partner Countries," dated June 14, 2004;
- Guidance from Staff Requirements Memorandum on SECY-14-0014, "Sharing of Safeguards Information with the International Atomic Energy Agency and other Multilateral Organizations," dated May 7, 2014; and
- Changes to Title 10 of the *Code of Federal Regulations*, Part 73, Section 22, that have been instituted since the previous publication of Management Directive 12.7 in 2008.

This revision also incorporates recommended changes resulting from Office of the Inspector General Audit OIG-12-A-12, "Protection of Safeguards Information," dated April 16, 2012, including the new reporting structure for one point of contact to report SGI release, the responsibility for the SGI release tracking system, and guidance on granting "outsiders" access to SGI and the incorporation of interim policy on the day-to-day safekeeping and storage of SGI.

TABLE OF CONTENTS

I. INTRODUCTION....3

A. Purpose and Scope....3
B. Applicability....4
C. Authority for the Control and Handling of Safeguards Information....4
D. Authority to Designate Safeguards Information....5
E. Release of Information to the Public....6
F. "No Comment Policy" for SGI....7
G. Safeguards Information in Official Agency Records....7
H. Handling Safeguards Information – Modified Handling (SGI-M)....7

II. THE PROTECTION AND CONTROL OF SAFEGUARDS INFORMATION ORIGINATED BY NRC AND NRC CONTRACTORS....7

A. Access....7
B. Sharing SGI with Foreign Entities....10
C. When Information is Marked as Safeguards Information....11
D. How Information is Marked....11
E. Cover Sheet....14
F. Reproduction....14
G. Non-Electronic Transmission....15
H. Preparation for Transmission....15
I. Electronic Transmission....16
J. Information Technology Processing....16
K. Protection During Use....16
L. Storage....16
M. Destruction of Safeguards Information....17
N. Residential Use....18
O. Telecommuting Policy....18
P. Use of Safeguards Information During Official Travel....18
Q. Removal of Information From the Safeguards Information Category....18
R. Reporting Inadvertent or Unauthorized Release of Safeguards Information....20
S. NRC Contractor Security Requirements....21

III. NRC DESIGNATION GUIDE FOR SAFEGUARDS INFORMATION (SGI)....22

A. Approval of the NRC Designation Guide for SGI....22

B. Review of the NRC Designation Guide for SGI 22
C. Dissemination of the NRC Designation Guide for SGI 22

IV. SAFEGUARDS INFORMATION (SGI) ORIGINATED BY SOURCES OTHER THAN THE NRC, NRC CONTRACTORS, AND NRC LICENSEES 22

V. HEARINGS, CONFERENCES, OR DISCUSSIONS ON SAFEGUARDS INFORMATION (SGI) 22

A. Security Preparations Required for Hearings, Conferences, or Discussions 22
B. Locations 23

EXHIBITS

Exhibit 1 Safeguards Information Cover Sheet and Document Marking 24
Exhibit 2 Safeguards Information Travel Procedures 26

I. INTRODUCTION

A. Purpose and Scope

1. The requirements and procedures set forth in Management Directive (MD) 12.7 provide assurance that Safeguards Information (SGI) is adequately protected from unauthorized disclosure. Specific procedures for the protection of SGI in information technology (IT) systems are contained in MD 12.5, “NRC Cyber Security Program.”

2. 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.

3. Further, SGI identifies a licensee’s or applicant’s detailed—

   (a) Security measures for the physical protection of special nuclear material, source material, or byproduct material;

(b) 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;

(c) Design features of the physical protection system;

(d) Operational procedures for the security organization;

(e) Improvements or upgrades to the security system;

(f) Vulnerabilities or weaknesses not yet corrected; and

(g) Any information as the Commission may designate by order.

4. Information may become SGI when the combination of components of non-SGI, in one document, provides enough information in the aggregate to become SGI even though the individual components of information do not meet the SGI threshold.

5. 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.

B. Applicability

1. NRC employees, consultants, and contractors are responsible for ensuring that the procedures specified in Sections I-II of this handbook are followed to protect SGI pursuant to Section 147 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.). The requirements of this MD will be imposed on contractors through the subject contract documents (see MD 11.1, "NRC Acquisition of Supplies and Services," for more information on security requirements for contract performance).

2. The use of "contractor" 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 the NRC.

C. Authority for the Control and Handling of Safeguards Information

Section 147 of the Atomic Energy Act of 1954, as amended, authorizes the Commission to issue such regulations or orders necessary to prohibit the unauthorized disclosure of SGI. The NRC regulations at Title 10 of the *Code of Federal Regulations* (10 CFR) 73.21 implement the Commission's authority.

D. Authority to Designate Safeguards Information

1. To obtain SGI designator authority, an NRC employee, contractor, or consultant must satisfy all of the following requirements:

   (a) Successfully complete the required SGI designator authority training, which is available on iLearn as "U.S. NRC's Safeguards Information and Designator Web-Based Training Course," and forward a copy of the training completion certificate to the Chief of the Information Security Branch (ISB), Division of Security Operations (DSO), Office of Nuclear Security and Incident Response (NSIR) (hereafter ISB, DSO, NSIR).

   (b) Forward the endorsed memorandum, with the subject line "Request for SGI Designator Authority," to ISB, DSO, NSIR. For NRC employees, the memorandum should be endorsed and submitted by the branch chief or higher. For contractors and consultants, the memorandum should be submitted by the respective branch chief, or higher, of the contracting officer's representative (COR). It is the responsibility of the requesting office to verify that the NRC employee, contractor, or consultant requires SGI designation authority to fulfill his or her duties for employment.

   (c) Receive certification as a SGI designator through ISB, DSO, NSIR. Upon notification of certification, the SGI designator will be authorized to make SGI determinations and have his or her name added to the SGI designator authority list.

2. Requests for SGI designator authority must be renewed annually, to include resubmission of the signed memorandum and completion of the "U.S. NRC's Safeguards Information and Designator Web-Based Training Course." An SGI designator will be notified through iLearn (within 30 days of the anniversary date of the certification) that refresher training is required to retain the SGI designator authority. If the training and signed memorandum are not submitted by the anniversary date of certification, the subject individual's SGI designator authority will be removed and his or her name removed from the list of authorized SGI designators.

3. Some SGI designators may also be identified as SGI designators within the Safeguards Information Local Area Network and Electronic Safe (SLES). In accordance with the SLES Operations Manual, inactive accounts will be disabled after 90 days of non-usage. The SLES Federal Program Manager will request that the user justify retention of the account and designator authority (if the user has authority to create, edit, designate, etc.). If the individual does not provide an affirmative response, the system administrators will disable the user's account and inform ISB, DSO, NSIR, that the subject individual's account, with SGI designator

authority, has been disabled. Based upon that notification, ISB, DSO, NSIR, will, in turn, contact the individual's branch chief and request an update as to the individual's need for retention of the SGI designator authority for day-to-day activities that do not involve SLES.

4. Each program office and region is required to have a sufficient number of SGI designators trained and certified to make SGI determinations.

E. Release of Information to the Public

1. 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 whether the document is releasable (see MD 3.4, "Release of Information to the Public").

2. Whenever an NRC individual has a question regarding the releasability of information, the employee should consult with his or her supervisor and contact the following offices:

   (a) The Information FOIA, Privacy, and Information Collections Branch, Office of Information Services (OIS), if a request for information involves the Freedom of Information Act (FOIA) (5 U.S.C. 552), Sensitive Unclassified Non-Safeguards Information (SUNSI), or the Privacy Act (5 U.S.C. 552a).

      (i) If the request relates to the NRC's general public health and safety mission, see MD 3.1, "Freedom of Information Act," MD 3.2, "Privacy Act," and MD 3.4, "Release of Information to the Public."

      (ii) For more information on SUNSI requirements, see MD 12.6, "NRC Sensitive Unclassified Information Security Program," as well as the "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information," which is available on the internal NRC Security Web site, at http://www.internal.nrc.gov/sunsi/pdf/SUNSI-Policy-Procedures.pdf, and NRC Yellow Announcement YA-05-0077, "Policy Revision: NRC Policy and Procedures for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information (SUNSI)," issued on October 26, 2005 (ML051220278).

   (b) DSO, NSIR, to determine whether a document contains SGI.

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

F. "No Comment Policy" for SGI

1. 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. Moreover, the fact that SGI appears in the public domain is in itself SGI that must be protected from public disclosure. An NRC employee, contractor, or consultant (i.e., personnel) who discovers SGI on public facing media should report the discovery using the procedures stated in Section II.R, "Reporting Inadvertent or Unauthorized Release of Safeguards Information," of this handbook. Additionally, personnel must be mindful that SGI is not permitted on the local area network and must not be discussed in areas not approved for SGI discussion. 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.
2. For further details regarding the "no comment" policy, contact DSO, NSIR.

G. Safeguards Information in Official Agency Records

SGI that is retained for official agency recordkeeping purposes may be stored only on systems and networks authorized for SGI processing in accordance with MD 12.5, "NRC Cyber Security Program." Do not use the Agencywide Documents Access and Management System (ADAMS) to store SGI. ADAMS is **not** approved for SGI (see MD 12.5, Handbook Section III.B.5(b)).

H. Handling Safeguards Information – Modified Handling (SGI-M)

Although information designated as "Safeguards Information – Modified Handling" (SGI-M) has modified handling requirements for licensees and 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.

II. THE PROTECTION AND CONTROL OF SAFEGUARDS INFORMATION ORIGINATED BY NRC AND NRC CONTRACTORS

A. Access

1. A security clearance is not required for access to SGI. However, except as the Commission may otherwise authorize, no person may have access to SGI unless that person has an established "need-to-know" (NTK) for the information and has undergone a Federal Bureau of Investigation (FBI) criminal history records check using the procedures set forth in 10 CFR 73.57. The NTK for SGI is met when a person having responsibility for protecting SGI determines that a proposed

recipient's access to SGI is necessary in the performance of official, contractual, or licensee duties of employment.

2. Additionally, for a person to be granted access to SGI, he or she must be deemed trustworthy and reliable based on a background check or other means approved by the Commission. The background check must include, at a minimum, an examination of the subject's employment history, education, and personal references as prescribed by 10 CFR 73.22(b)(2). Certain categories of personnel are exempt from the aforementioned FBI criminal history records check and other elements of the background check requirements; see Section II.A.8 of this handbook.

3. Occasionally, staff may need to share SGI with personnel from another Federal or State agency. In all instances however, the intended recipient must meet the minimum access requirements prescribed by 10 CFR 73.22(b). When the intended recipient of SGI states that he or she has an active Federal security clearance, no additional fingerprinting or background check is required as the probative scope associated with an active Federal security clearance meets the fingerprinting requirements and other elements of the background check that are prescribed by 10 CFR 73.22(b). When relying upon an existing active Federal security clearance to meet the SGI access requirements, excluding the NTK determination requirement, staff must first coordinate with the Office of Administration (ADM), Division of Facilities and Security (DFS), to verify the existence of the requestor's active Federal security clearance.

4. When a non-NRC employee, contractor, and/or consultant, i.e., an intervener, vendor, external stakeholder or member of the general public (hereafter referred to as "outsiders") request access to SGI, the regional or program office that received the request shall either make a NTK determination (if it is the SGI originating office or the office that has primary interest in the information), or seek the assistance of DSO, NSIR for guidance with the identification of an appropriate NTK determination official. All NTK determinations for access to SGI by outsiders **must** be made with the concurrence of the regional or program office management (i.e., branch chief or above). When the NTK determination is made in association with an NRC adjudicatory proceeding, staff must follow the procedures outlined in 10 CFR 73.22(b)(4).

5. If the requester's NTK is affirmed, the sponsoring regional or program office shall contact DFS, ADM, and inform that office of its desire to grant SGI access to an outsider, then request DFS, ADM, assistance with ensuring that the requester meets the regulatory requirements for access to SGI.

6. The outsider may be denied access to SGI on the basis of the review and adjudication of the applicant's (outsider's) fingerprint criminal history records check;

submitted security forms that were deemed necessary by DFS, ADM; or adverse information received by DFS, ADM. Once all required information has been received and due process applied, DFS, ADM, will notify the requesting regional or program office of the decision to grant or deny the request for SGI access.

7. When SGI is shared with an outsider, the responsible regional or program office will ensure that—

   (a) The access takes place on NRC property.

   (b) The outsider remains under direct observation while possessing SGI.

   (c) The outsider is not allowed to duplicate or record the SGI, unless otherwise approved.

   (d) The outsider is not allowed to remove the SGI from the NRC facility unless approved by regional or program office management, in coordination with and the approval of DFS, ADM.

8. In accordance with 10 CFR 73.59, the following categories of individuals are exempt from the aforementioned access procedures. However, they must possess a NTK and must adhere to the SGI protection requirements prescribed by 10 CFR 73.22:

   (a) An employee of the Commission or the Executive Branch of the United States Government who has undergone fingerprinting for a prior U.S. Government criminal history records check;

   (b) A member of Congress;

   (c) An employee of a member of Congress or congressional committee who has undergone fingerprinting for a prior U.S. Government criminal history records check;

   (d) The Comptroller General or an employee of that Government Accountability Office who has undergone fingerprinting for a prior U.S Government criminal history records check;

   (e) The Governor of a State or his or her designated State employee representative;

   (f) 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, including SGI designated as SGI-M;

   (g) Federal, State, and local law enforcement personnel;

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

(i) 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;

(j) 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;

(k) Any agent, contractor, or consultant of the aforementioned persons who has undergone equivalent criminal history records and background checks to those required by 10 CFR 73.22(b) or 73.23(b); and

(l) A Tribal official or the Tribal official's designated representative, and Tribal law enforcement personnel.

9. 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.

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

B. Sharing SGI with Foreign Entities

1. It has been the policy of the NRC to share SGI with foreign regulatory counterparts or other foreign government entities with whom it has signed an Arrangement of Cooperation (Arrangement) for the exchange of technical information and, subsequently, with whom the Commission has approved staff to share SGI. Following the receipt of a request for SGI from a foreign government entity with whom NRC has signed an Arrangement, the Director of the Office of International Programs (OIP) will—

   (a) Make a net advantage determination; and

   (b) Initiate a NTK assessment in coordination with affected program offices.

2. After it is determined that the requesting entity has a NTK, OIP will request permission from the Commission, by memorandum, to release the SGI. OIP will list the information to be released, the timing of the proposed release, the recipient of the information, and the outcome of the net advantage determination by the Director of OIP. After the Commission has approved the request to share SGI, no further

Commission approval is required for other SGI requests from that foreign entity for a period of 5 years. During the 5-year period after the Commission's approval, OIP will notify the Commission, in writing through a Commissioners' Assistant Note (CA Note), of any additional SGI requests made by that entity before sharing additional SGI with that entity. OIP will be required again to seek Commission approval for requests to share SGI received after the 5-year period has expired for a particular entity, before sharing SGI with that foreign entity.

3. This guidance does not apply to the sharing of SGI that includes design basis threat (DBT) information or aircraft impact assessment-related information. Staff must request Commission approval, in each instance, prior to sharing SGI that includes aircraft impact assessment-related information. Similarly, Commission approval must be sought prior to the sharing of SGI with multilateral organizations, and prior to the exchange of SGI with the IAEA outside IAEA activities conducted under the U.S./IAEA Safeguards Agreement.

4. Prior to the actual sharing of SGI with visiting foreign entities, OIP will obtain assurance from the recipient's government entity that the representatives of that entity are qualified to receive and protect SGI. Note: This guidance does not apply to the foreign assignee program. Guidance on the foreign assignee program can be found in MD 12.3, "NRC Personnel Security Program."

5. OIP will coordinate with ISB, DSO, NSIR, to arrange a brief presentation that informs the intended recipient of the sensitivity of the information and the information security requirements according to U.S. laws and regulations, including the AEA of 1954, as amended, and 10 CFR 73.21.

C. When Information is Marked as Safeguards Information

Information in any form (e.g., electronic or hard copy) containing SGI must be marked accordingly. See Exhibit 1, "Safeguards Information Cover Sheet and Document Marking," and the internal NRC Security Web site at https://adamsxt.nrc.gov/WorkplaceXT/IBMgetContent?objectStoreName=Main._.Library&vsId={3ACAD171-512C-4F5C-A786-1C55852AE5D9}&objectType=document, for additional guidance and examples.

D. How Information is Marked

1. Safeguards Information Designators

   At the time it is determined that a document contains SGI, regardless of the amount (i.e., portion, paragraph, bullet or sub-bullet), SGI designators must—

   (a) Mark each document to indicate the presence of SGI or SGI-M in a conspicuous manner on the top and bottom of each page with the words "Safeguards

Information" or "Safeguards Information-Modified Handling" (preferably in a font larger than that used in the body of the document). 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;

(ii) The date the determination was made; and

(iii) A marking that unauthorized disclosure will be subject to civil and criminal sanctions.

(b) Ensure that 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 SGI enclosure(s), this document is decontrolled"). If the transmittal letter or memoranda contains SUNSI, the document shall be marked to indicate that the attachment or enclosure(s) contain SGI, but that the transmittal document does not (i.e., "When separated from Safeguards Information enclosure(s), this document shall be controlled as (Official Use Only – Security-Related Information, Official Use Only – Sensitive Internal Information, etc.")).

(c) Ensure that any transmittal document or other matter forwarding SGI alerts 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.

(d) Ensure that the 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.

2. Multiple-page Documents

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

(a) The outside of the front cover, if any;

(b) The first page;

(c) Each internal page of a document containing SGI; and

(d) The back page or cover.

3. Portion-Marking

   (a) Portion-marking is accomplished by clearly indicating the portions (e.g., titles, paragraphs, bullets, sub-bullets, subjects, or pages) that contain SGI by placing the abbreviation “SGI” or “SGI-M” in parentheses at the beginning of the portion.

   (b) Portion-marking is required when—

      (i) A document contains several categories of SUNSI in order to distinguish SGI portions (e.g., paragraphs, pages, and appendices) from other portions containing other SUNSI, including personally identifiable information (PII) and other SUNSI information. In such cases, SGI or SGI-M would be the overall marking used at the top and bottom of the page.

      (ii) 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 Sections II - IV of this handbook.

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

      (i) In cases where portions are segmented such as paragraphs, sub-paragraphs, bullets, and sub-bullets and the designation level is the same throughout, it is sufficient to put only one portion marking at the beginning of the main paragraph or main bullet.

      (ii) If there are different designation levels of information among segments, then all segments shall be portion marked separately in order to avoid over-designation of any one segment.

      (iii) If the information contained in a sub-paragraph or sub-bullet is a higher level of designation than its parent paragraph or parent bullet, that will not change the designation of the parent paragraph or parent bullet so that both are designated at that same level (e.g., the sub-bullet may be a higher designation than the parent bullet, which remains at a lower level of designation).

4. Files or Folders

   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.

5. Other Media Containing Safeguards Information

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

E. Cover Sheet

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 this handbook) to facilitate identification and protection of the information.

F. Reproduction

1. Documents that contain SGI may be reproduced in accordance with MD 12.5, "NRC Cyber Security Program," 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. Paper jams shall be immediately cleared. All copies must clearly show the protective markings contained on the original document. See MD 12.5, Handbook Section VI.C.6, for additional guidance on copying, and 10 CFR 73.22(e). Copiers used to reproduce SGI must be evaluated to ensure that unauthorized individuals cannot access SGI. Those evaluated copiers must be approved by DFS, ADM, and must be located within a space that is approved by DFS, ADM.

2. 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).

3. If reproduction services for SGI are requested, the requestor must properly communicate the proper handling and disposal. The requestor must submit an NRC Form 20, "Request for Printing and Copying Services," which is available on the NRC Forms Library in SharePoint, to be completed as follows:

   (a) The requester shall explain in the special instructions block that SGI is attached, and an asterisk shall be placed in the "Unclassified" and "Other" blocks.

   (b) 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) These actions described in Sections II.F.3(a)-(b) of this handbook must be taken to ensure proper handling of the document and proper disposal of any waste (see Sections II.L and II.M of this handbook).

G. Non-Electronic Transmission

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

   (a) Within NRC headquarters facilities: NRC interoffice mail in two opaque envelopes.

   (b) Outside NRC, to include NRC regional facilities: 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 tracking capability.

   (c) Hand-carried by any individual authorized access to SGI, as based on approval from the employee's division director or designee.

   (d) Outside the continental United States: By government-to-government mail channels or approved electronic means.

   (e) Other means approved by the Director of DFS, ADM.

2. 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).

H. Preparation for Transmission

1. The inner envelope or wrapper must have the words "Safeguards Information" at the top and bottom on both sides and be addressed to the intended recipient, with a return address included. 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 steel locking bar and a three positions, changeable combination, GSA-approved padlock.

2. When preparing documents containing SGI for transmission outside an NRC facility or an NRC contractor facility in accordance with the means identified in Section II.G of this handbook, 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 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

address of the sender, and must not bear any markings or indication that the document or other matter contains SGI.

3. Guidance to the postmaster should be placed beneath the return address. For example, the guidance “POSTMASTER: Do Not Forward, Return to Sender” should be sufficient to ensure that the SGI is not forwarded to an address other than that appearing on the envelope or container.

I. Electronic Transmission

1. All routine electronic transmissions of SGI must be transmitted using technologies in accordance with MD 12.5.
2. Approval for the use of specific hardware or software security procedures implementing transmission protection of SGI resides with the Computer Security Office (CSO) as described in MD 12.5. Staff must coordinate with CSO to address the security plans and other documentation used for certification/accreditation of protective measures.
3. 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 Director of DSO, NSIR; to the Director of CSO; and to the Director of DFS, ADM.
4. SGI may not be processed into ADAMS (see MD 12.5, Handbook Section III.B.5(b)).

J. Information Technology Processing

SGI must be processed in accordance with MD 12.5. Note: SGI must not be disclosed during social media activities in accordance with the agency’s social media policy (ML103060402).

K. Protection During Use

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

L. Storage

1. SGI must be stored in either a GSA-approved security container or a file cabinet equipped with a steel locking bar and a three positions, changeable combination, GSA-approved padlock when unattended or not in actual use, except as authorized in an area approved by DFS, ADM.

2. SGI may be stored electronically in the Safeguards Information Local Area Network and Electronic Safe (SLES).

3. As the term is used in Section II of this handbook, “security storage container” includes any of the following containers:

   (a) 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;

   (b) 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”;

   (c) A bank safe deposit box; or

   (d) Other containers approved in writing by the Director of DFS, ADM.

4. The lock combinations protecting SGI must be limited to a minimum number of persons who have a NTK to conduct official business and are otherwise authorized access to them in accordance with the provisions of this MD. Combinations must be changed when first placed in use, when access by an authorized person is no longer required, when a combination has been the subject of a possible unauthorized disclosure, when a security incident involving an SGI container left unsecure occurs, or once every 3 years if none of the other items above occur. Contact DFS, ADM, to change the combination.

5. 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, and reported to DFS, ADM.

M. Destruction of Safeguards Information

1. Holders of SGI documents are responsible for destroying these documents when they are no longer needed or required to be maintained.

2. SGI must be destroyed using methods of destruction that preclude reconstruction (i.e., shredding or burning). Pieces no wider than 1/4 inch, composed of several pages or documents and thoroughly mixed, are considered completely destroyed. The pieces should not exceed 1/4 inch when measured either vertically or horizontally. Destruction methods that have been approved for classified information are also acceptable for the destruction of SGI. Electronic media that contains SGI must be marked in accordance with MD 12.5 and Computer Security Office Standard 2004 (CSO-STD 2004), “Electronic Media and Device Handling Standard,” and destroyed or cleaned as described in MD 12.5 or sent to DFS, ADM, for

destruction. For information on the management and handling of removable electronic media, see MD 12.5, Handbook Section III.B.5.b(ii), and Section 3.2 of Computer Security Office Standard CSO-STD 2004.

3. Destruction records for SGI are not required.

N. Residential Use

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

O. Telecommuting Policy

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

P. Use of Safeguards Information During Official Travel

1. Use of SGI during official travel by NRC employees is not generally authorized since other means of advance transmission (e.g., mail and secure facsimile) are usually available except as authorized in NRC's SGI Travel Procedures (see Exhibit 2 to this handbook).
2. 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. The employee's division director or designee will approve, in writing, the handling and storage of SGI during official travel and will provide a copy to DFS, ADM.
3. Procedures for NRC employees or contractors handling SGI while on official travel are described in Exhibit 2 to this handbook.

Q. Removal of Information From the Safeguards Information Category

1. 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 FOIA or the Privacy Act would necessitate a review of this type.

(b) 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.

2. Who May Remove Information From the SGI Category

(a) 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 10 CFR Part 73, provided the following individuals are informed:

(i) The individual who originally determined that the document contained SGI or his or her successor; and

(ii) A supervisor of either of the above individuals (branch chief or higher level official) or other individual identified in writing by the office director or regional administrator of the office or region who made the original SGI determination.

(b) If there is a disagreement over a change of categories, the procedure set forth in Section II.Q.4 of this handbook must be followed.

3. Marking

(a) When Information Is Marked

The following is the required marking to indicate that a document has been removed from the SGI category. This marking shall appear in a prominent location on the document.

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

(Signature of person making determination)	(Title)	(Office)	(Date)

(b) Change in Category

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

(c) Removal of Markings

(i) 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.

(ii) 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.

(iii) 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.

4. Disagreement on Changes of Category

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.

R. Reporting Inadvertent or Unauthorized Release of Safeguards Information

1. All security incidents involving SGI (computer security related or facilities security related), despite the means by which they occur must be immediately (within 1 hour) reported by one of the following methods:

(a) Select the “report a security incident” button on the upper right-hand corner of the NRC internal Web site.

(b) Contact the security incident reporting hotline on (301) 415-6666. Contractor employees shall immediately notify the COR that an incident has occurred, the details of the incident, and the name of the person(s) involved.

2. When security incidents involve unprotected SGI, the person or persons that discover that information should (1) immediately take possession of it, (2) notify his

or her (their) immediate supervisor or guard force member, and (3) take steps to protect it from unauthorized disclosure. In instances where SGI is discovered on a public-facing Web site or other media that is publicly available, personnel should report the discovery of that information using one of the methods referenced above in Section II.R.1 of this handbook.

3. Because information concerning a security incident may contain SGI, all personnel are required to discuss, document, or otherwise process incident information in accordance with information protection requirements for SGI. Specifically, when communicating about security incidents involving the loss or possible compromise of SGI, NRC staff, consultants, and contractors must be attentive of the content of e-mail communications and the location of verbal communications related to the loss or possible compromise of that information so as not to cause additional damage or unauthorized disclosure.

4. After initial report of the security incident, the affected program office must ensure that corrective measures are immediately implemented pending the implementation of a long-term resolution. Additionally, the affected program office must complete and forward NRC Form 183, “Report of Security Incident,” to DFS, ADM. The completed NRC Form 183 should not contain SGI unless necessary to adequately report the security incident. Note: If SGI is to be included within the NRC Form 183, it must not be completed or stored on the LAN. The affected program office then must manually complete NRC Form 183 (i.e., handwritten, or by an electronic means prescribed by MD 12.5).

5. All reported security incidents will be followed-up by DFS, ADM, with a preliminary inquiry. Once the preliminary inquiry has been completed, DFS, ADM, may issue a memorandum to the appropriate program office for long-term follow-up actions. Referrals to the Office of the Inspector General (OIG) and OIG’s associated investigative role are unaffected by the policy in this MD.

S. NRC Contractor Security Requirements

1. NRC offices and divisions must promptly notify DFS, ADM, of their intent to initiate a contract involving access to or possession of SGI. The COR must submit a completed NRC Form 187, “Contract Security and/or Classification Requirements,” with the statement of work to DFS, ADM; the COR must also provide a copy to DSO, NSIR. Work on any contract (or purchase order) involving SGI cannot commence before approval by DFS, ADM.

2. Contractors desiring onsite possession of SGI are subject to security inspections to determine eligibility to store and handle SGI. Contractor statements of work that may require access to SGI are submitted by the Acquisition Management Division,

ADM, to the Director of DFS, ADM, and a copy provided to the Director of DSO, NSIR, in accordance with MD 11.1. Work on any contract or purchase order involving SGI cannot commence prior to written approval by the Director of DFS, ADM. See MD 12.5 for electronic processing of SGI.

III. NRC DESIGNATION GUIDE FOR SAFEGUARDS INFORMATION (SGI)

NRC DG-SGI-1, "NRC Designation Guide for Safeguards Information," is available on the NRC internal Web site, at http://nsir.nrc.gov/pdf/Designation%20Guide%20for%20Safeguards%20Information.pdf, or in hard copy from ISB, DSO, NSIR.

A. Approval of the NRC Designation Guide for SGI

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

B. Review of the NRC Designation Guide for SGI

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

C. Dissemination of the NRC Designation Guide for SGI

The NRC Designation Guide for SGI is an Official Use Only document, and shall be distributed as widely as necessary and in accordance with the NRC policy to ensure proper awareness.

IV. SAFEGUARDS INFORMATION (SGI) ORIGINATED BY SOURCES OTHER THAN THE NRC, NRC CONTRACTORS, AND NRC LICENSEES

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 II of this handbook.

V. HEARINGS, CONFERENCES, OR DISCUSSIONS ON SAFEGUARDS INFORMATION (SGI)

A. Security Preparations Required for Hearings, Conferences, or Discussions

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—

1. Provide to DFS, ADM, a verified list of attendees who have authorized access to SGI before an SGI event is held at an NRC facility.

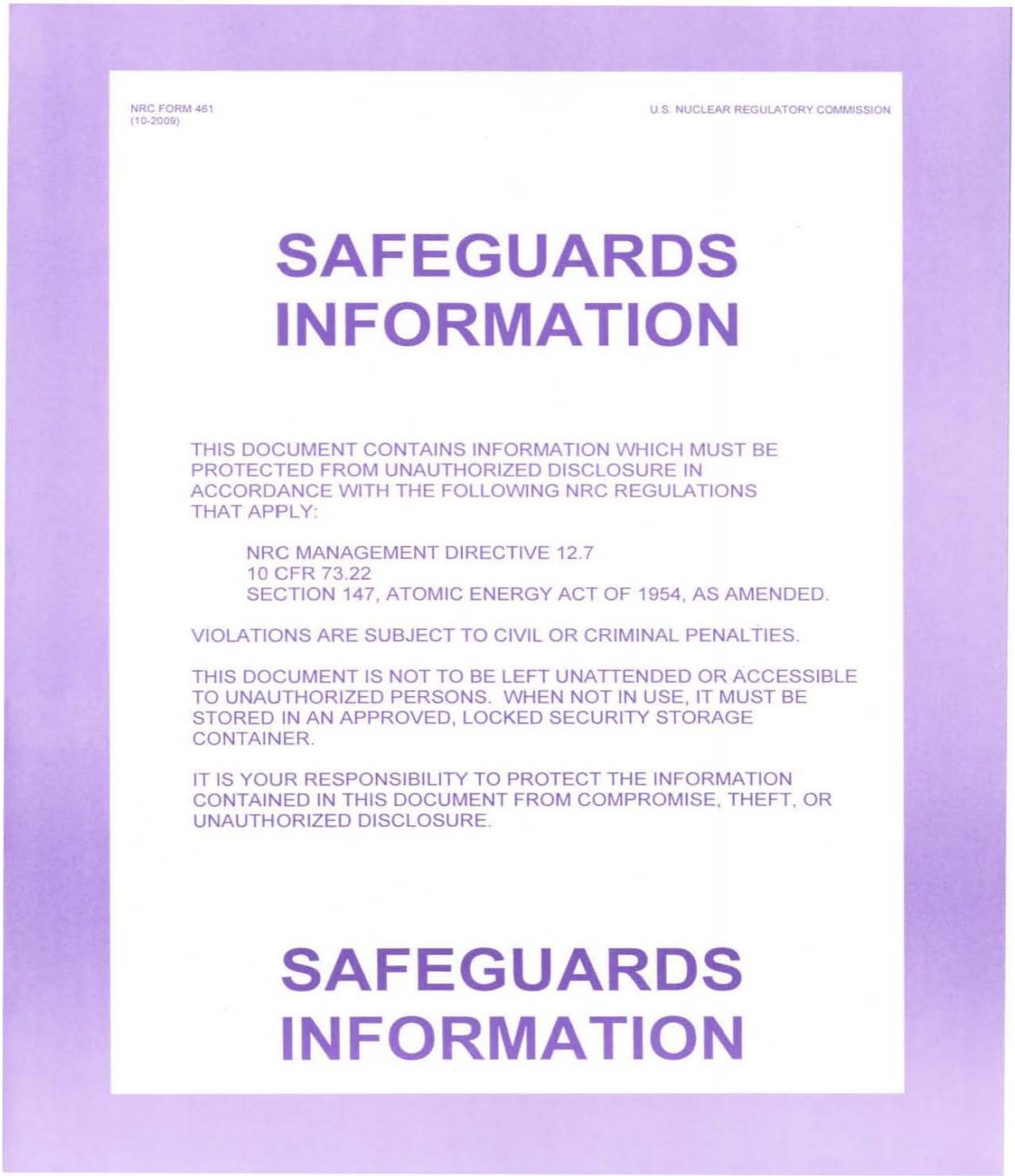
2. Ensure that all attendees are pre-registered in the Visitor Access Request System by the meeting point of contact for any SGI event held at an NRC facility.
3. Coordinate with DFS, ADM, a minimum of 10 days before any SGI event (i.e., hearings, conferences, or discussions) occurring at an NRC facility to ensure that the room has been approved by DFS, ADM, for SGI discussions and establish any additional security requirements for the event.
4. Ensure before a hearing, conference, or discussion that participating personnel are identified and are authorized to have access to the information to be discussed.
5. Indicate to participating personnel that the specific information they will receive is SGI and advise them of the protective measures, as prescribed by 10 CFR 73.22(b)-(i) that are required.
6. Ensure that no discussion takes place that is audible or visible to persons not authorized access to the information.
7. Ensure that electronic devices that have not been authorized to process SGI (e.g., cellular telephones, tablets, laptops) are not permitted in the meeting room.

B. Locations

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 of guarded or controlled areas only when DFS, ADM, is consulted for the purposes of obtaining appropriate guidance for the physical protection of SGI.

EXHIBITS

Exhibit 1 Safeguards Information Cover Sheet and Document Marking



NRC FORM 461
(10-2009)

U.S. NUCLEAR REGULATORY COMMISSION

SAFEGUARDS INFORMATION

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

NRC MANAGEMENT DIRECTIVE 12.7
10 CFR 73.22
SECTION 147, ATOMIC ENERGY ACT OF 1954, 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 AN APPROVED, 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 Safeguards Information Cover Sheet and Document Marking (continued)

NRC REQUIRED MARKINGS:

SAFEGUARDS INFORMATION (SGI)

SAFEGUARDS INFORMATION
Subject (U)

(SGI) XXXXX
(U) XXXXX
(SGI) XXXXX

SAFEGUARDS INFORMATION

Overall page marking top and bottom - all pages

Portion marking

First Page Only

WARNING: Violation of Section 147 of the Atomic Energy Act, "Safeguards Information" is subject to Civil and Criminal Penalties

First Page Only

Safeguards Information determination made by:
Name/Title _____
Organization _____
Basis _____
Signature _____ Date _____

ACCESS:	Meets the requirements of 10 CFR 73.22 (b), NRC Management Directive 12.7, or other NRC requirements, **and** has a need-to-know.
STORAGE:	In an approved, locked security storage container when not in use. See Management Directive 12.7, Part II, "Storage," or alternative NRC guidance for more information on approved security storage containers.
MAIL:	USPS first class, registered, express, certified, overnight mail, or a commercial carrier with computer tracking features.
WRAPPING:	Use two opaque envelopes, mark inner envelope "Safeguards Information" on both sides, top and bottom; include the address and identification of intended recipient. The outer envelope must have the recipient address and sender's return address. **Do not** indicate the level of information contained within, 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 or later.
ELECTRONIC SYSTEMS:	Process **only** on a "stand-alone" PC, a PC physically disconnected from the Local Area Network (LAN) with a removable hard drive (**Note:** the operating system and application software must reside on the removable hard drive); or over an approved network (e.g., FIPS 140-2 compliant) that limits access to SGI authorized personnel.
ADAMS:	**Do not** enter documents containing Safeguards Information into ADAMS. Transmittal documents may go into ADAMS without the SGI enclosure **if they do not themselves contain SGI**.

For more detailed information on these topics, consult NRC Management Directive 12.7 and 10 CFR 73.22.

10/2009

Exhibit 2 Safeguards Information Travel Procedures

General Policy

Use of SGI during official travel for NRC employees and contractors is not generally authorized because other means of advance transmission (e.g., 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: The approving official notifies DFS, ADM, of instances in which SGI is handled or stored by employees during official travel.)

A. Pre-departure

1. Written approval must be obtained in advance from a division director or his or her designee to possess and use SGI during official travel. Additionally, the approving official shall notify DFS, ADM, of his or her decision in advance of travel.
2. 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 nor available.
3. 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 ISB, DSO, NSIR, until the need to hand-carry SGI on official travel is terminated.
4. 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.
5. Electronic media that contains SGI must be labeled and used in accordance with MD 12.5 and Computer Security Office Standard 2004 (CSO-STD 2004), “Electronic Media and Device Handling Standard.”

B. In-use While on Travel

1. 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 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, ADM, should be consulted/informed for guidance.

2. If none of these options are available, the traveler must retain positive control of the information at all times.
3. 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

Electronic SGI must be processed, stored, and marked in accordance with MD 12.5.

D. Reproduction of SGI

SGI must be reproduced in accordance with established CSO procedures as prescribed by MD 12.5.

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:

1. 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.
2. 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.
3. If, upon producing the letter, airport security personnel still insist on opening the SGI package, the traveler should not intervene further.

F. Reporting

All security incidents involving SGI (computer security related or facilities security related), despite the means by which they occur must be immediately (within 1 hour) reported by one of the following methods:

1. Select the "report a security incident" button on the upper right-hand corner of the NRC internal Web site.

2. Contact the security incident reporting hotline on (301) 415-6666. Contractor employees shall immediately notify the COR that an incident has occurred, the details of the incident, and the name of the person(s) involved. Upon return from official travel, unless directed otherwise, the traveler must complete and submit an NRC Form 183 “Report of Security Incident,” to DFS, ADM, for follow-up actions.