Nuclear Regulatory Commission Guide for Designation of Safeguards Information

January 29, 2004

draft

Table of Contents

Intent

The guidance and criteria in this document pertain to the protection of Safeguards Information (SGI) as described in the Atomic Energy Act of 1954, as amended (AEA). The AEA authorizes the Nuclear Regulatory Commission (NRC) to prescribe requirements by regulation or order to prohibit the unauthorized disclosure of SGI. It is intended to assist NRC staff, licensees and other persons in properly identifying and designating such information in order to ensure its protection in accordance the AEA.

The NRC intends to strike a balance between the public's right to information so they can meaningfully participate in regulatory processes and the need to protect sensitive security information from inadvertent release or unauthorized disclosure which might compromise the security of nuclear facilities or materials. All persons who have or have had access to SGI have a continuing obligation to protect SGI against inadvertent release and unauthorized disclosure.

The terrorists attacks of September 11, 2001 prompted NRC to re-evaluate the terrorist threat to radioactive materials in the United States. As part of NRC's efforts to enhance security following 2001, NRC expanded application of SGI protection, for example, on June 6, 2003, the NRC issued orders to panoramic and underwater irradiators to enhance security measures. The enhanced security measures imposed by order were necessary to protect significant quantities of radioactive material and have been designated as SGI. Although this information is subject to the same protection authority under the AEA as information previously designated SGI, NRC recognized that the potential adverse consequences of unauthorized disclosure are less than other types of information protected as SGI. This information has been designated as Safeguards Information - Modified (SGI-M).

The NRC will continue to evaluate its requirements, policies and guidance concerning the protection and unauthorized disclosure of SGI. Licensees and other stakeholders will be informed of proposed revisions or clarifications.

Introduction

SGI is a special category of sensitive unclassified information authorized by Section 147 of the AEA to be protected. Although SGI is sensitive unclassified information, it is protected more like government classified confidential information than like other sensitive unclassified information (*e.g*., privacy and proprietary information). Access to SGI requires a valid need-to-know and an authorization by a competent authority based on the trustworthiness and reliability of the individual receiving the SGI. The authorization is normally obtained based on a background check or other means to verify an individual's character.

The criteria for designating special nuclear material and power reactor information as SGI and associated restrictions on access to and protection of SGI are codified in Title 10 of the *Code of Federal Regulations,* Part 73, Section 73.21 (10 CFR 73.21). Part 73 applies to licensees and/or applicants for operating power reactors, research and test reactors, advanced technology reactors, decommissioning facilities, transporting of irradiated reactor fuel, fuel cycle facilities, and spent fuel storage installations. NRC has also designated SGI and the associated handling requirements in NRC Orders for other users of radioactive material.

SGI is officially 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. For the purpose of common defense and security, this would include Agreement State licensees. The unauthorized release of this information, for example, could result in harm to the public health and safety; 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.

Further, SGI broadly identifies a licensee's or applicant's (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) the design features of the physical protection system; (4) operational procedures for the security organization; (5) required improvements or upgrades to the security system; (6) vulnerabilities or weaknesses not yet corrected; and (7) such other information as the Commission may designate by order.

Access to SGI requires authorization and applies to anyone who has an established "need to know" for the information and is authorized by the Commission or falls under any of the categories listed in 10 CFR 73.21(c)(1) sections (i) through (vi). SGI must be appropriately designated and withheld from public disclosure. It must also be physically controlled and protected. Physical protection requirements include (1) secure storage, (2) document marking, (3) restricted access, (4) limited reproduction, (5) secure transmission, and (6) enhanced automatic data processing system controls.

Applicability

Any person who produces, receives, or acquires SGI is subject to the requirements (and sanctions) of the Atomic Energy Act of 1954, as amended. Firms and their employees that supply services or equipment considered important to the protection of commercially used radioactive material would fall under the rule. Licensees or others responsible for the protection of SGI must also inform contractors and suppliers of the existence of the regulatory requirements and the need for proper protection. Inadequate protection of SGI, including inadvertent release or unauthorized disclosure, may result in civil and/or criminal penalties. The Act explicitly provides in Section 147a that any person, whether or not a licensee of the Commission, who violates any regulations adopted under this section shall be subject to the civil monetary penalties of section 234 of the Act. Furthermore, willful violation of any regulation or order governing SGI is a felony subject to criminal penalties in the form of fines or imprisonment, or both, as prescribed in section 223 of the Act.

Distinction from other types of information

Public Information

Information relating to security measures is typically not considered SGI, if the information is legitimately in the public domain. Information published or discussed by entities not authorized access to SGI cannot be designated as SGI, if the information was obtained or developed without the assistance of an SGI authorized individual. The fact that sensitive or classified information has appeared publicly is itself protected at the same level as the information in question by the NRC. In addition, the fact that information has appeared publicly does not render the information "unclassified or decontrolled." Therefore, any questions raised about the accuracy, designation/classification, or technical merit of such information should be responded to in a "no comment" manner; that is, the NRC or other entity will neither confirm nor deny the presence of SGI or classified information." Such information would not be acknowledged by authorized parties as SGI and is covered by a "no comment" policy. General information developed by the NRC may be designated as SGI if such information is required to address vulnerabilities in a licensees' program for protection of radioactive materials. Upon completion of upgrades, the designation of such protective measures may be considered for removal from the SGI category if it does not reveal other facilities that have not completed upgrades.

Information, developed by a licensee, of a general nature and not specific to a particular facility is usually not SGI unless it includes studies of the impacts on nuclear facilities or radioactive materials from postulated security events or information that would disclose generic vulnerabilities to a class of facilities or material user. Normal engineering or construction drawings that show the locations of safety-related equipment are not SGI. Another example would be security measures identified by the NRC as necessary to improve security at licensees. Generally, the specificity of the information and its usefulness to defeating security measures at a particular facility increases the likelihood that it will be useful to an adversary and should be considered SGI. The overall measure for consideration of SGI is the usefulness of the information (security or otherwise) to an adversary in planning or attempting a malevolent act.

General information concerning State or local police forces, such as total complement, shift size etc., that is already in the public domain is not SGI and not subject to protection under the AEA.

Other types of information not considered as SGI:

-Documents, drawings, or reports submitted by applicants or licensees, or produced by the staff, in response to the environmental and safety requirements contained in Parts 50, 51, 70, and 71

-Routes and quantities for spent fuel shipments (specific dates and times are SGI)

-Information concerning licensee control and accounting procedures or inventory differences for source material or byproduct material

-Any information already in the public domain including commercial safeguards equipment specifications, catalogues and equipment buying data

-Portions of guard qualification and training plans that do not disclose facility safeguards features, response procedures, or other information not designated by NRC as SGI.

-Information related to Category I facilities

-Environmental or geological information

Classified Information

Classified information at the NRC and at the facilities it regulates is primarily of two categories: (1) **National Security Information** (NSI): information classified under the National Security Act and in accordance with an Executive Order, whose compromise would cause some degree of damage to the national security; and (2) **Restricted Data** (RD): information classified by the Atomic Energy Act, whose compromise would assist in the design, manufacture, or utilization of nuclear energy for military purposes.

Licensees for commercial power reactors, research and test reactors, and other radioactive materials do not generally handle Restricted Data and have access to NSI on a very limited basis.

Possession of classified information requires a specific government national security clearance and a “need-to-know.” Classified information is withheld from public disclosure. After September 11, 2001, the NRC has arranged for a small number of personnel from licensed commercial nuclear power reactors and other facilities to obtain clearances for possession of classified information. This program was developed to allow the NRC or other Government agencies to provide information to licensees about potential threats as needed. Applicable Federal laws and regulations govern the controls for preventing the release of classified information.

The NRC may classify information about a facility even if the facility is not a national security facility, depending upon the nature of the information and its relevance to national security.

10 CFR 2.790(d) Information

Information about a licensee's or applicant's physical protection or material control and accounting program for special nuclear material not designated as SGI or classified as National Security Information or Restricted Data is required by 10 CFR 2.790(d) to be protected in the same manner as commercial or financial information, i.e., they are exempt from public disclosure.

There is some information related to security at NRC licensed facilities that warrants withholding from public disclosure, although it does not meet the existing criteria for designation as SGI. This type of information was recognized before September 11, 2001, and, when submitted to the NRC by a licensee, is withheld from public disclosure according to the provisions of 10 CFR 2.790(d)(1). This regulation states:

(D) The following information shall be deemed to be commercial or financial information within the meaning of §9.17(a)(4) of this chapter and shall be subject to disclosure only in accordance with the provisions of §9.19 of this chapter. (1) Correspondence and reports to or from the NRC which contain information or records concerning a licensee's or applicant's physical protection, classified matter protection, or material control and accounting program for special nuclear material not otherwise designated as SGI or classified as National Security Information or Restricted Data.

Types of Information to be designated as SGI
SGI is sensitive unclassified information that has intrinsic security value involving equipment, procedures, communications, analyses, design basis, or response plans used by a licensee or applicant to protect certain special nuclear material, byproduct material, source material, or facilities. It includes, but is not limited to, the following:

-The overall physical security and safeguards contingency plan for a nuclear power reactor

- Drawings, sketches and diagrams that show location of site safeguards features not readily observed by public means or observation

-Details of the intrusion alarm system

-Guard orders and procedures

-Details of on-site and off-site response forces

-Response and patrol routes

-Communications equipment and protocols (locations of backups, etc.)

-Drawings that explicitly identify certain areas or equipment at power reactors as being vital for purposes of physical protection

-Portions of guard training and qualification plans that disclose specific safeguards features or response procedures

-Correspondence, inspection reports and audits that contain any of the above or that disclose weaknesses in the protection system

-Uncorrected vulnerabilities or deficiencies of actual implementation when compared against requirement

-Generic studies, guidance, reports or analyses conducted by or on behalf of the NRC, licensees, or applicants that would disclose capabilities or vulnerabilities of security measures for nuclear materials or facilities

-Media other than paper documents and drawings that contain SGI, such as alarm system computer programs, data processing storage disks, microfilm or photographs

Normally the composite (i.e., sum of all parts) physical security and safeguards contingency plans would be considered single entities for protection purposes. However, licensees and applicants may find it more appropriate to segregate general or non-sensitive information into unprotected appendices or attachments. Also, guard orders and standard operating procedures may be segregated into protected and unprotected portions. (Note that 73.21 requires guards qualification and training plans to be segregated)

In regard to engineering or construction drawings, all the revisions that substantially represent the final design features of the physical protection system would be considered SGI. Initial requests for bids or proposals and original design sketches, for examples would probably not be designated as SGI. Specific design items designated as SGI would include:

- Location and types of alarm devices

-Alarm system schematic and wiring diagrams (but not wiring lists) to include Closed Circuit Television (CCTV) including Pan, Tilt, Zoom and fixed cameras, locations and power sources

-Defensive positions and guard posts

-Alarm system emergency power location and capability

-Communications equipment (specific to facility)

-Details of alarm station and security post bullet resistant construction features

-Location of alarm stations (when it does not conflict with other submittal requirements)

-Vehicle alarm and immobilization features

In addition to physical protection measures, the NRC requires protection of documents or drawings that identify certain safety related equipment as being vital for the purpose of physical security. In order to be SGI, the drawing must explicitly state that the equipment or area is vital from the standpoint of physical protection. **(Unless a drawing is specifically made, overlaid, or annotated for purpose of the physical protection of the facility, it is not considered SGI.)**

Arrangements made with State or local police forces for response to safeguards emergencies are SGI. Specific information to be protected include:

-Size and armament of initial responding force

-Response times

-Primary and alternate routes

-Identity (e.g., Does the response force come from a road unit or HQ building which allows response times and capabilities to be estimated or known)

-Specific response plans upon arrival

-Availability of reserve forces

-Communication protocols and methods

Specific Guidance
The remainder of this guide provides specific guidance for use by knowledgeable reviewers and designators of SGI on the types of information that warrant protection of SGI. Designation of documents is most effective when appropriate markings are applied. These markings identify the appropriate designation levels and alert the recipient of a document as to proper handling precautions. The following symbols are used in this designation guide:

U	Undesignated or decontrolled information. No markings are required by this guide. It is possible that information in this category may be Official Use Only or other type of unclassified sensitive information such as 10 CFR 2.790(d) commercial or financial information and protected from public disclosure by the Freedom of Information Act.
2.790(d)	Information relating to a licensee's or applicant's physical security or material control and accounting information program not otherwise designated as SGI, National Security Information, or Restricted Data.
SGI	Safeguards Infomation. Depending on licensee type, this information will be marked as SGI for special nuclear material licensees or as *Safeguards Information-Modified Handling* (SGI-M) for byproduct and source material licensees.
C	Confidential. Information classified by Statute and/or Presidential Executive Order, the unauthorized disclosure of which could cause damage to the National Security.
S	Secret. Information classified by Statute and/or Presidential Executive Order, the unauthorized disclosure of which would cause severe damage to the National Security.
TS	Top Secret. Information classified by Statute and/or Presidential Executive Order, the unauthorized disclosure of which would cause exceptionally grave damage to the National Security.

NSI National Security Information. Classified category marking authorized by Presidential Executive Order 12958, as amended. Primarily deals with physical security or vulnerability information.

RD Restricted Data. Classified category marking authorized by Atomic Energy Act of 1946, as amended. Primarily deals with technology information important to the nation's nuclear weapons program.

Safeguards Information Categories

SGI is protected from public release by exemptions of the Freedom of Information Act (FOIA). Specifically, exemption three of the FOIA regulations addresses the type of information covered by SGI as authorized by the Atomic Energy Act of 1954, as amended (information exempted by statute). The marking stamp designating a document or media as SGI should also be accompanied by an indication of which SGI functional area the document addresses. Specific marking instructions are included in NRC Management Directive 12.6, "NRC Sensitive Unclassified Information Security Program." Functional areas include:

1. Program Management
2. Research and Development
3. Physical Protection Program
4. Vulnerabilities, Threats, and Scenarios
5. Incidents of Security Concern
6. Plant Operations and Emergency Planning

The inclusion of these functional areas in the SGI marking will aid others in understanding the overall SGI marking and for what reason the document was determined to receive protection as an SGI document. These markings as well as portion marking of documents will assist in understanding the reasons for why a particular document was designated as SGI.

REMOVAL FROM SGI CATEGORY

SGI is exempt from automatic decontrol and does not require markings to indicate when information is no longer required to be protected. This is similar to how Restricted Data documents are handled.

However, documents or other media containing SGI can be removed from the category if, and when, they no longer contain information defined by this guide or the event or situation no longer can be of any use to a potential adversary in harming the common defense and security. Examples of this include: security events that have passed with proper security measures in place to prevent recurrence; outdated security measures that bear no resemblance to current measures; or vulnerabilities that no longer exist. Decontrol or removal of information from the SGI category should be accomplished by marking through the SGI markings on the media and signature by an authorized individual that the information is no longer SGI. If feasible, notification of other holders/recipients of the document should be made with a request that they

decontrol their copy as well. Although beneficial to other holders of the SGI media, it is not required to determine the whereabouts of other copies of the media or verify that the information has been revised accordingly. Such information would remain protected at the higher level until removed from the category or destroyed. In many cases, destruction of media is preferred to removal unless document control measures require otherwise.

1 PROGRAM MANAGEMENT

Broad Guidance
It is NRC's mission to ensure protection of commercial facilities with radioactive material assets important to the health and safety or common defense and security of the United States. Accordingly, program and planning information is SGI if it reveals information that would aid or encourage an adversary to attack a commercial facility or radioactive material. Information concerning NRC general requirements as described in NRC regulations and orders is undesignated as SGI unless it reveals information designated by this or other applicable guidance. Currently, none of the NRC regulations is designated as SGI. Some NRC orders relating to physical security of nuclear facilities have been designated as SGI due to the specificity of the information and the potential for disclosing vulnerabilities. Information concerning NRC minimum requirements for the various aspects of the information security program is not designated as SGI. Actual implementation of these requirements may be SGI as detailed in the other sections and chapters of this guide.

1.1 Program Planning, Management and Administration

Information revealing NRC requirements for Safeguards & Security (S&S)

As delineated in non-safeguards NRC Orders and regulations **U**

As delineated in SGI Orders **SGI**

Information concerning the NRC S&S program organizational structure **U**

Information concerning the implementation of the NRC S&S program **U**

NOTE: Unclassified unless the details of the implementation are SGI

1.2 Documents and Findings

1.2.1 NRC Related Documents and Correspondence

Security enhancements such as Additional Security Measures (ASMs formerly called Interim Compensatory Measures (ICMs) or Compensatory Measures (CMs)) issued by the NRC for facilities or radioactive material other than National Security facilities **SGI**

NOTE: Information may be decontrolled after completion of security enhancements if it would not reveal a vulnerability.

Documents/correspondence addressing less than adequate implementation or performance related to ASMs **SGI**

1.2.2 Information revealing time lines or schedules for future implementation for security related items

General information about NRC deadlines/timelines as specified in publicly available documents **U**

Timelines or schedules indicating noncompliance with NRC required implementation (Dependent upon identification of vulnerability) **U-SGI**

1.2.3 Information contained in Security Plans

Results of vulnerability assessments, response tactics, and other security details contained in security plans **SGI**

For detailed guidance, see topics on vulnerabilities and other pertinent information addressed in other sections of this guide.

1.2.4 Capabilities

Specific capabilities, such as Special Weapons and Tactics (SWAT) or explosives ordnance disposal teams, (onsite and offsite) that could aid an adversary in selecting targets or planning malevolent acts. **SGI**

Capabilities of safeguards or security equipment, site specific values or custom specifications **SGI**

1.2.5 Procedures

Complete protective force procedures **SGI**

Individual procedures regarding security measures that would significantly aid an adversary in obtaining radioactive material or defeating security systems. **SGI**

1.2.6 Security Budget Information

Budget information not indicating security system design deficiencies **U**

As built, or “off the shelf” systems **U**

Ancillary budget information indicating safeguards and security system design vulnerabilities **SGI**

1.2.7 Inspections, Audits and Evaluations

Portions of security inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system. **SGI**

Note: Information regarding defects, weaknesses or vulnerabilities may be released after corrections have been made. Reports of investigations may be released after the investigation has been completed, unless withheld pursuant to other authorities, e.g., the Freedom of Information Act (5 U.S.C. 552).

Time frame and date of planned exercise regarding a standard shift (8 or 12 hour) or start and end times of the exercise **SGI**

Attack scenarios, details and analysis **SGI**

Vulnerabilities, determined or assessed **SGI**

1.2.8 Training and Qualifications

Complete protective force training plans or programs **SGI**

Individual sections or details of training plans or programs describing specific capabilities or vulnerabilities (An event basis for decontrol may exist once vulnerabilities are corrected or mitigated) **SGI**

1.2.9 Foreign Ownership, Control, or Influence (FOCI)

1.2.9.1 FOCI process

Identification of licensees, applicants, or contractors whose FOCI determinations are current or in progress **U**

Fact of annual review and/or certifications and most details concerning the routine FOCI process, except information concerning anomalies and subsequent actions **U**

Final determination of FOCI review action **U**

Fact of approval/disapproval, no elaboration **U**

Identification of FOCI topical element(s) causing disapproval, without elaboration **2.790(d)**

Identification of FOCI topical element(s) causing disapproval, with elaboration **2.790(d)**

May be classified if elaboration is based on classified information

1.2.9.2 Anomalies

Fact that an anomaly occurred in the investigative/review process **May be 2.790(d)**

Criteria/rationale for conducting investigations of anomalies **U-SNSI**

NOTE: Classification level is based on classification guidance from the investigating agency.

Methodology for conducting investigations of anomalies **U-SNSI**

NOTE: Classification level is based on classification guidance from the investigating agency.

2 RESEARCH AND DEVELOPMENT

Broad Guidance
Software or information which could be used by an adversary to understand the methodology used by NRC to protect civilian radioactive material is SGI and should not be publicly released. Software or information that could be used by an adversary to analyze a security system in order to understand its strengths and weaknesses is clearly SGI. Methodology and modeling of adversary/protective forces provide great insight into security design for facilities handling significant quantities of radioactive materials. Such models may reveal vulnerabilities such as pathways into a facility with elements of intrusion detection and delay that allow an adversary to achieve an objective in less time than required for a security response.

Information generated by facility assessment programs is typically very technical in nature and addresses topics like security system design, performance limits, and vulnerabilities. This type of information may provide a considerable advantage to an adversary attempting to defeat or circumvent operational security systems and should therefore be protected.

2.1 General information about protection programs

Undesignated or decontrolled information providing general concepts and approaches for how elements of a system will be or are designed and integrated to produce an effective security system (e.g., general reliance on intrusion detection, assessment, and responses) **U**

Design information about a protection program capability under development having a goal or objective of significantly improving the performance of an existing capability, especially when it corrects or mitigates a vulnerability **SGI**

Design information about a protection capability that is intended to protect against a threat not mitigated by existing protection systems	**SGI**
Operational/conceptual scenarios of how a protection capability under development may be used to enhance a protection program system	**SGI**
Titles, goals and/or objectives of projects being sponsored by a technology development program	**U**
Evaluations which reveal design, procedural, or operational details which could significantly assist an adversary	**SGI**
Design information and evaluations that reveal a vulnerability	**SGI**

2.2 Information concerning equipment or protection system performance

Probability of detection	
Statement of compliance with NRC requirements	**U**
Manufacturer's published performance, tolerances, data, etc.	**U**
Values actually used in vulnerability assessment reports and the association with specific equipment	**SGI**
Probability of neutralization or interruption	
Values actually used in vulnerability assessment reports and the association with specific equipment	**SGI**
NOTE: Values that are in the open literature become SGI when used in vulnerability assessments.	
Reliability of a protection capability that discloses a vulnerability	**SGI**
Amount of delay time used in a vulnerability assessment that a specified security barrier provides against a specific threat *NOTE*: Values that are in the open literature are SGI when used in vulnerability assessments.	**SGI**

Time required for a specified attack tool to make a passable opening in a specified, significant barrier *NOTE*: Values that are in the open literature are SGI when used in vulnerability assessments.	**SGI**
2.3 Software and/or information about risk analysis and system modeling	
The fact that NRC, licensees, or applicants have assessed security system performance or the general approach for such analyses	**U**
Software or information concerning methodology used by NRC to protect nuclear sites or to analyze an NRC safeguards or security system in order to understand its strengths and weaknesses	
Without site specific data, but considered useful to an adversary	**SGI**
With site specific data	**SGI**
Simulation software that would allow an adversary to predict the outcome of an attack on a licensed facility or radioactive material, or to conduct "war-gaming" exercises	
Without site specific data, but considered useful to an adversary	**SGI**
With site specific data	**SGI**
2.4 Technical advances	
Not related to security system performance (e.g., improvements such as cost effectiveness or user friendliness which have little or no impact on site risk calculations)	**U**
Primarily related to security system performance (e.g., improvements in factors such as probability of detection, probability of interruption or probability of neutralization significantly impacting site risk calculations)	**SGI**
To mitigate a vulnerability for which no other solution exists	**SGI**
In the design or performance of Special Nuclear Material (SNM) tamper indicating seals and tags not revealing how they may be defeated	**U**

2.5 Technical deficiencies

Details concerning a deficiency in a technology that is not commercially available	**U-SGI**

NOTE: Designation is dependent upon vulnerability criteria

2.6 Design solutions for deficiencies

Solutions requiring a technology that is not commercially available

Fact that a solution exists	**U**
Details about the solution	**SGI**

Solutions for a technology that is commercially available

Fact that a solution exists	**U**
Details about the solution	**SGI**

3 PHYSICAL PROTECTION PROGRAM

3.1 Security Force Operations

3.1.1 Response

Detailed information concerning tactics and capabilities beyond that described in NRC regulations or Regulatory Guides	**SGI**
Specific training and qualifications of protective personnel beyond that described in 10 CFR Part 73, or in Regulatory Guides	**SGI**
Number of protective personnel at a facility (armed or otherwise)	**U**
Number of protective personnel on a given shift (armed or otherwise)	**U**
Number of dedicated, armed responders who will respond in a given contingency	**SGI**

3.2 Security Systems

3.2.1 Facility/Site Features

Information concerning overall site, facility, or security areas revealing security deficiencies, weaknesses, or concerns that is not readily determined by casual observation from an uncontrolled area **SGI**

3.2.2 Equipment

Detailed Information concerning security equipment and/or procedures that could aid an adversary in selecting a specific target(s) or developing an attack strategy **SGI**

Information concerning security equipment deficiencies **SGI**

Information concerning equipment failure to meet required performance criteria **SGI**

Location of concealed alarms or security equipment **SGI**

Site or facility specific details of installation (wiring diagrams, locations, redundancy) **SGI**

Evaluations of equipment revealing deficiencies or vulnerabilities (e.g., failure rates, excessive maintenance, inadequate coverage, limitations) **SGI**

Specific keys, locks, combinations, passwords, and codes as used for security purposes **SGI**

3.3 Access Controls

Access controls, details derived from publicly available means or observable from outside security controlled area **U**

Access controls, details not observable from outside security controlled area **SGI**

Access control program (hardware and software), including locations and layouts, detailed descriptions **SGI**

Personal Identification Numbers (PINs) and passwords required for access while access is authorized **SGI**

4 VULNERABILITIES, THREATS, AND SCENARIOS

Broad Guidance
The Design Basis Threat (DBT) set of criteria that NRC uses for evaluating security systems, actual details concerning a specific threat, and the basis for the DBT are considered SGI. Such DBT information can also be classified depending on source or facility. NRC has issued general descriptions of the DBT that are not designated as SGI or National Security Information

(NSI) such as the description in 10 CFR 73.1. Site safeguards and security designs of intrusion detection and assessment, barrier delays, response force size and capabilities, and communications are based on the DBT. Obviously, many reactions to a given threat condition are observable and simply may not represent SGI or classified information. The designation or classification of emerging threats would be based on the source of information and analysis that identified the emerging threat. Vulnerabilities and detailed scenarios revealing information that would significantly assist an adversary in planning or committing a malevolent act would be considered SGI.

4.1 Threat, Intelligence, or Law Enforcement Information

Adversary characteristics as described in 10 CFR Part 73 **U**

Any tactical attribute of the Designed Basis Threat beyond characteristics described in 10 CFR Part 73, in whole or in part **SGI**

NOTE: DBT for theft or diversion is classified

Threat or intelligence information received from official sources causing facility self-assessment to verify or dismiss threat such as an ongoing search for explosives or material **U-SGI**

Note: Depends on level of detail regarding the information source and extent to which knowledge of the information describes a vulnerability

Actions required to ensure health and safety in response to threat or intelligence information such as evacuations **U**

Specific actions required to ensure physical protection of material or facility in response to threat or intelligence information **SGI**

4.2 Vulnerabilities

Information concerning security plans and procedures provided this information cannot be obtained by casual observation from uncontrolled areas **SGI**

Information revealing vulnerabilities of a specified security plan, procedure, or system **SGI**

The fact that a specified facility, or activity, has an unspecified security vulnerability that does not jeopardize overall effectiveness **U**

Information concerning a security vulnerability at an unspecified facility or activity at an unspecified site which does not reveal in any way the identity of the sensitive facility or activity **U**

Physical security features or measures (uncompensated) that are not meeting performance requirements **SGI**

Failed or degraded protection features (uncompensated) for nuclear material or vital equipment **SGI**

Measures designed to protect nuclear materials or facilities contemplated or not fully implemented (e.g., access programs, equipment upgrades, security configurations) **SGI**

Identification of weaknesses or vulnerabilities in a security system that could be exploited by an adversary **SGI**

Detailed cost or budget information indicating safeguards and security system design vulnerabilities **SGI**

Scenarios considered sufficient to defeat security measures for a facility **SGI**

Ongoing investigation or review of potential weakness/vulnerability in safeguards or security system **SGI**

Statements by knowledgeable individuals (e.g., security supervisors, security force members, NRC inspectors, industry representatives) detailing weaknesses or vulnerabilities in a safeguards or security system **SGI**

Reports of loss, suspected loss, compromise, or potential compromise of SGI, unevaluated or uncompensated **U-SGI**

Note: Generally, reports are not SGI if they do not reveal details that could be exploited (e.g., 50.72 requirements)

4.3 Threat description as stated in the DBT

Fact that the threat is defined (no elaboration) **U**

Number of adversaries (outside/inside) **SGI**

Motives addressed in the DBT (politics, revenge, sabotage, theft, etc.) **U**

Level of the threat's capabilities, equipment, training, or knowledge

General (e.g., as described in NRC regulations) **U**

Detailed (e.g., as described in NRC SGI Orders) **SGI**

Elaboration of DBT used for facility security design or testing **SGI**

NOTE: An elaboration of the DBT would include the following elements: facility, number of adversaries, specific weapons, specific type and weight of explosive charges and other breaching tools, and arrival and departure mode of transportation.

4.4 Actual threats

4.4.1 Generic threat information not related to the DBT or actual threat information

NOTE: Generic threat information has no relationship to the DBT or actual threats. **U**

4.4.2 Evaluations of emerging threats

NOTE: Classify based on the guidance used by the government agency responsible for the threat. **U-TSNSI**

4.5 Threat messages (from a perpetrator)

4.5.1 Non-nuclear threat messages

Fact that a non-nuclear threat message has been received **U**

Information in a non-nuclear threat message

NOTE: Classification designation is based on information content. **U-TSNSI**

Fact that a non-nuclear threat message contains classified information **SGI (May be classified)**

4.5.2 Nuclear threat messages

Fact that a nuclear threat message has been received

By the NRC or other agency **SGI (May be classified)**

Fact that a specific nuclear threat message contains classified information **SGI**

Use of information from a classified nuclear threat message **SGI (May be classified)**

Information in a nuclear threat message **Classified by originating agency**

4.6 Data bases used for assessment

NOTE: Designate information consistent with the control/classification of individual terms and associations included. **U-SGI (May be classified)**

Compilation concept. A series of non-SGI documents or pieces of information when combined forma viable description of methods, techniques, or information advantageous to an adversary. **SGI**

4.7 Specific Vulnerability Analyses

4.7.1 General

Fact that an analysis of a facility has been conducted concerning the potential consequences resulting from the hypothetical attack.	**U**
The specific spent fuel storage cask designs proposed for use in a facility.	**U**
Design and engineering information (including calculations) related to spent fuel storage cask designs concerning the structural design of casks, material information (type, yield strength, etc.), and accident analysis (e.g., tornado missile). NOTE: Design and engineering information and related safety analyses may contain proprietary information.	**U**

4.7.2 Specific

Specific input parameters such as analysis methods or codes used in analysis (Generally, such codes or methods are unclassified and publicly available). NOTE: If code or analysis method is classified, then consult NRC classification authority and classify according to level of input information. This guidance is not intended for facilities containing classified materials or performing classified activities.	**U**
Specific input parameters for attack such as length, weight, structure, range, top speeds, or altitude of an aircraft, that are easily obtained through publicly available sources.	**U**
Specific output results (when separated from the analysis) that provide general information and do not disclose vulnerabilities.	**U**
Specific input parameters of the attack, unique to the analysis, not obtained from public sources (e.g., angle of attack, designated impact speed of aircraft, location of attack).	**SGI**
Specific analysis (entire document or discussion) including input parameters, analysis methods or codes, output results, and consequences.	**SGI**

Specific analytical information (when adverse consequences are not identified) that can be reverse engineered by an adversary to gain an exploitable advantage (e.g., information on the margin of safety to yield strength or initiation of a radiological release, relative to an attack scenario that could be used to plan a successful attack). **SGI**

4.7.3 Analysis Results or Consequences

Specific output results where the consequences show that a material confinement boundary (target container or building) remains intact. **SGI**

Fact that no adverse consequences concerning radioactive material releases have been identified from the postulated attack. **U**

Fact that adverse consequences or vulnerabilities have been identified from the postulated attack that could result in a release of radioactive material in comparison with a dose standard (e.g., 10 CFR72.106). **SGI**

Specific output results where the consequences or vulnerabilities show that a the radioactive material confinement boundary does not remain intact and is evaluated against a specific standard. **SGI**

4.8 Vulnerabilities

Unspecified Vulnerability

Authoritative information that no vulnerability or major vulnerability exists at a site or facility **U**

At nuclear facilities in general **U**

At a designated facility or for a class of facilities or material user (Classified if applies to a classified facility or operation) **SGI**

In a designated component [essential element(s)] of a specified security system - facility specific or class of facilities or material user **SGI**

In administrative procedures or in command, control, and communications in NRC Headquarters or Regions **U**

In administrative procedures or in command, control, and communications at a designated facility or class of facilities or material user **SGI**

In external arrangements, local law enforcement agency back-up, or legal authorities (force, pursuit, etc.) for a specific site or class of facilities or material user **SGI**

In defending against a specified attack (e.g., sabotage of a critical facility or radioactive material theft) at a designated facility or class of facilities or material user **SGI**

In defending against a type of attack consistent with Design Basis Threat - facility specified or specific class of facilities or material user **SGI**

Complete or partial scenarios of an attack - site or facility specified or unspecified (fact of existence) **SGI**

The fact that analyses of security (physical, computer, nuclear material accounting, etc.) system show the system is vulnerable to a successful attack - specified or unspecified facility **SGI**

NRC and/or licensee-sponsored vulnerability assessments of facilities or class of facilities that disclose vulnerabilities **SGI**

Results of NRC or licensee-sponsored vulnerability assessments showing no vulnerabilities **U**

NOTE: SGI if a vulnerability is revealed and security is impacted.

4.9 Essential system elements

NOTE: For any scenario, an essential system element(s) is a single element (or set of elements) of a security system whose defeat is sufficient for an adversary to successfully attack the asset being protected by the security system.

Information revealing methods or techniques that are sufficient for defeating a set of essential system elements of a security system that could result in gaining unauthorized access to controlled access areas **SGI**

Compilation concept. A series of non-SGI documents or pieces of information when combined form a viable description of methods, techniques, or information advantageous to an adversary. **SGI**

Unclassified information revealing details of minor discrepancies or inadequacies of no substantial impact (e.g., the fact that equipment calibration is overdue or that there is minor erosion at a fence) **U**

Information revealing methods or techniques that are either necessary or sufficient to defeat a nonessential system element(s) of a security system **SGI**

4.10 Scenarios

Information in scenarios that is sufficient to defeat essential element(s) of the system or the total system protecting a nuclear facility **SGI**

Information in a scenario that is sufficient to defeat essential element(s) of the security system protecting a nuclear facility **SGI**

Information in scenarios that is not sufficient to defeat essential element(s) of the security system **U**

Information in a scenario that reveals methods or techniques that are sufficient to defeat a nonessential system element(s) of a security system **U**

Authoritative information that a specified vulnerability has been corrected and no longer exists at a designated facility **U**

NOTE: The information is designated at the level of the information or matter protected until it is determined that the vulnerability does not exist at other facilities or sites.

Fact that a specified site has not adequately evaluated a specified threat **SGI**

Comparisons or ranking according to vulnerability or estimated consequences of a successful attack **SGI**

NOTE: A comparison or ranking of sites or facilities is not equivalent to a rating as a result of an inspection or force-on-force exercise.

Fact without elaboration that a specified facility received negative findings as a result of a survey or inspection **U**

5 INCIDENTS OF SECURITY NONCOMPLIANCE

Broad Guidance
Most information concerning inquiry and investigative activities concerning licensee security programs and vulnerabilities is SGI. For example, information is SGI if it allows anyone to locate and obtain unsecured information about licensee security programs, that would be useful to an adversary. Information showing vulnerabilities that allows an unauthorized individual to gain access to radioactive materials or anyone to perform other malevolent acts is designated as SGI due to its potential to harm the public health and safety and/or the common defense and security.

Noncompliances involving information sent over the Internet, published in the news media, or entered into a database may be located through many different associations, including the subject of the information, association of a facility, the date of the possible compromise, the originator, or recipient of the information raises special concerns regarding potential compromise. The lack of security over the Internet is well publicized. Also, the likelihood of adversarial intercepts over telecommunications circuits raises concerns. For these reasons, sanitization of the sender's and receiver's computers, telecommunications equipment, and facsimile equipment shall not be considered sufficient to ensure that compromise has not occurred or that further compromise will not occur.

Topics in this section also apply to security incidents where SGI is communicated to an unauthorized recipient.

5.1 General

Descriptions of, or the occurrence of, potential compromise of SGI via inadequately protected e-mail, telephone, facsimile, or mail if general and does not disclose a vulnerability **U**

NOTE: One cannot be assured that a compromise has not occurred for email, telephone or facsimile transmission. Prior to release of such information after the fact, care should be given to whether the information can be exploited after the transmission (e.g., voicemail message, retrieval of facsimile)
Descriptions of potential compromise of SGI that could be exploited to recover SGI

Date of occurrence
With time of day unspecified **U**
With time of day specified **SGI**
Occurrence by specified individual or organization
With date unspecified **U**
With date specified **SGI**
Name of any attached e-mail files **SGI**
Description of the information compromised
General **U**
Specific, detailed **SGI**

Fact of FBI involvement
Fact that the FBI investigates significant incidents of security concern associated with NRC facilities **U**

Fact that the FBI is involved in an unspecified or a specified investigation at a specified facility (Designate according to FBI authority)

5.2 MISSING SGI

5.2.1 Fact of missing or uncontrolled matter

If the statement would materially aid an adversary in locating the SGI **SGI**

Fact of missing unidentified SGI **U**

5.2.2 Actual or potential compromise of SGI

Fact that a specified NRC, NRC contractor or subcontractor organization is conducting an inquiry into possible compromise of safeguards information **U**

CAUTION: If intelligence or counterintelligence activities are involved, other classification guides may apply and the fact of an inquiry may be classified.
Information providing the identity of a document or information that may have been compromised or providing the nature of the compromised information

If there is reason to believe that a compromise has occurred or can occur **SGI**

If it is reasonably certain, prior to completion of the inquiry, that no compromise has occurred or can occur **U**

If the inquiry is completed and it confirms with reasonable certainty no compromise occurred **U**

Facility name where the incident occurred or facilities affected by the incident **U**

Identification of inquiry officials and assisting personnel **U**

Date incident occurred **U**

Notifications made concerning the incident, within NRC and otherwise **U**

Actual information compromised or potentially compromised **SGI**

Fact that an identified document published in the open literature is being considered for designation review **SGI**

Fact that an identified document published in the open literature contains SGI **SGI**

5.3 Operations Security

5.3.1 Operations security threat

General statement of a threat revealing no more than the mere fact that adversaries are collecting information concerning NRC and licensee programs, operations, and activities **U**

Statements of threat that provide greater details, especially if related to a specific facility **SGI**
(May be classified depending upon source)

5.4 Automated Information Systems

5.4.1 Security analyses

Descriptions of vulnerabilities if general and do not reveal exploitable details **U**

Descriptions of means for defeating or bypassing system-specific AIS security measures **SGI**

Analyses (including risk analyses) revealing vulnerabilities in AIS security systems that could provide significant assistance for defeating or bypassing security measures **SGI**

5.4.2 Incident information

Fact of a suspected or attempted attack on a specific AIS containing SGI

When the fact reveals a vulnerability **SGI**

When the fact does not reveal a vulnerability **U**

Details of suspected or attempted (successful or unsuccessful) attacks on a specified AIS **SGI**

5.4.3 Vulnerabilities

Widely known information regarding an AIS vulnerability in specified hardware or software derived from open sources external to NRC and its contractors **U**

6 PLANT OPERATIONS AND EMERGENCY PLANNING

Contingency or Emergency Planning

Contingency planning information as used for security response **SGI**

Otherwise **U**

7 ACRONYMS

AEA	Atomic Energy Act of 1954, as amended
AIS	Automated Information Systems
ASMs	Additional Security Measures formerly called Interim Compensatory Measures (ICMs) or Compensatory Measures (CMs)
C	Confidential. Information classified by Statute and/or Presidential Executive Order, the unauthorized disclosure of which could cause damage to the National Security.
CCTV	Closed Circuit Television
CFR	*Code of Federal Regulations*
DBT	Design Basis Threat
FOIA	Freedom of Information Act
PINs	Personal Identification Numbers
NRC	Nuclear Regulatory Commission
NSI	National Security Information. Classified category marking authorized by Presidential Executive Order 12958, as amended. Primarily deals with physical security or vulnerability information
RD	Restricted Data. Classified category marking authorized by Atomic Energy Act of 1946, as amended. Primarily deals with technology information important to the nation's nuclear weapons program.
S	Secret. Information classified by Statute and/or Presidential Executive Order, the unauthorized disclosure of which would cause severe damage to the National Security.
S&S	Safeguards & Security
SWAT	Special Weapons and Tactics
SNM	Special Nuclear Material
SGI-M	Safeguards Information - Modified
SGI	Safeguards Infomation. Depending on licensee type, this information will be marked as SGI for special nuclear material licensees or as *Safeguards Information-Modified Handling* (SGI-M) for byproduct and source material licensees.

TS	Top Secret. Information classified by Statute and/or Presidential Executive Order, the unauthorized disclosure of which would cause exceptionally grave damage to the National Security.
U	Undesignated or decontrolled information. No markings are required by this guide. It is possible that information in this category may be Official Use Only or other type of unclassified sensitive information such as 10 CFR 2.790(d) commercial or financial information and protected from public disclosure by the Freedom of Information Act.
2.790(d)	Information relating to a licensee's or applicant's physical security or material control and accounting information program not otherwise designated as SGI, National Security Information, or Restricted Data.

ML040290787