

Safeguards Information (SGI) Awareness Training



U.S. Nuclear Regulatory Commission



Atomic Energy Act

Describes Safeguards Information (SGI) as a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act, of 1954, as amended. SGI must be protected from unauthorized disclosure.



Definition

SGL is information that is not National Security Information or Restricted Data. It's information that specifically identifies a NRC licensee's detailed:

- 1) Security measures for the physical protection of source, byproduct, or special nuclear material, or
- 2) Security measures for the physical protection and location of certain plant equipment vital to the safety of NRC licensed facilities

See 10 CFR 73.2



NRC Requirements

The criteria for designating special nuclear material and power reactor information as SGI, restricting access to it, and the protections for SGI are codified in Section 73.22 of Title 10 of the *Code of Federal Regulations* (10 CFR 73.22)



Who is covered by the Atomic Energy Act?

Any person, whether or not a licensee of the NRC, who produces, receives, or acquires SGI is subject to the requirements (and sanctions) of the Atomic Energy Act of 1954, as amended

See 10 CFR 73.21



Penalties for Unauthorized Disclosure

Inadequate protection of SGI, including inadvertent release or unauthorized disclosure, can result in civil and/or criminal penalties (The Atomic Energy Act)

See the Atomic Energy Act of 1954, as amended, Section 147



Penalties for Unauthorized Disclosure

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

See the Atomic Energy Act of 1954, as amended, Section 147



Conditions for Access

Access to SGI requires both a “need-to-know” and a determination that the proposed recipient is trustworthy and reliable. This is normally accomplished through a FBI fingerprint criminal history records check and a background check.

Background check examines

- Employment History
- Education
- Personal References

See 10 CFR 73.22(b)



Background Check Exemptions

Fingerprinting, and the identification and criminal history records checks required by Section 149 of the Atomic Energy Act of 1954, as amended, and other elements of background checks are not required for the following individuals prior to granting access to SGI as defined in 10 CFR 73.2:

- Tribal officials or the Tribal official’s designated representative and Tribal law enforcement personnel

Note: Despite exemption from the fingerprint and background check requirement, a “need-to-know” determination must be made prior to granting access to SGI

See 10 CFR 73.59(l)



Need-to-Know

A determination by a person having responsibility for protecting SGI (typically the person possessing the SGI) that a proposed recipient's access is necessary for the performance of official, contractual, or licensee duties of employment

See 10 CFR 73.22(b)



Tribal Official Expected Interactions with SGI

- Take receipt
- Review/Use
- Storage
- Reproduce
- Share/Transmit
- Destroy

See 10 CFR 71.97 and 73.37



Protection Requirements

While in Use

Under the control of an authorized individual

Requirement is satisfied if the SGI is attended by an authorized individual even though the information is, in fact, not constantly being used (SGI Cover Sheet or other method to shield the text should be used)

See 10 CFR 73.22(c)



Protection Requirements

While in Storage

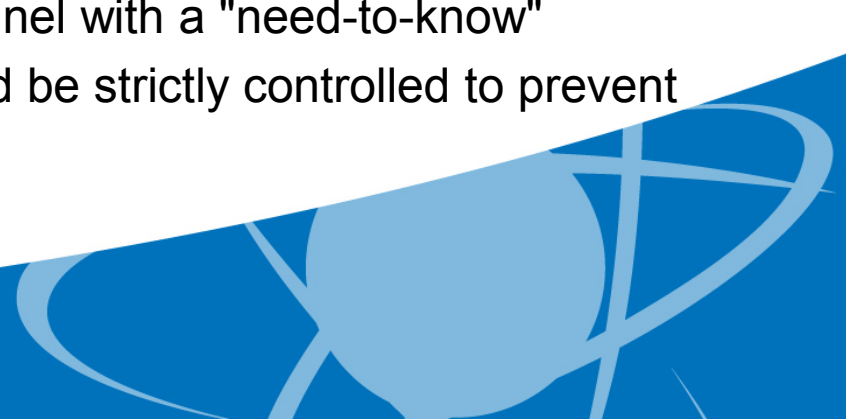
Stored in an approved security storage container

- Within a protected or controlled access area:
 - a steel filing cabinet equipped with a steel locking bar and a 3-position, changeable combination, General Services Administration (GSA) approved padlock
- Outside of a protected or controlled access area:
 - A Security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or interior place, and is marked GSA Approved Security Container

Knowledge of lock combinations or access to keys protecting SGI should be limited to a minimum number of authorized personnel with a "need-to-know"

Access to lock combinations or keys should be strictly controlled to prevent unauthorized disclosure of information

See 10 CFR 73.22(c)



Transportation of SGI Documents

Outside of facility

When transported outside an authorized place of use or storage

- Enclosed in two sealed envelopes or wrappers

Inner envelope or wrapper contains the name and address of the intended recipient, marked both sides, top and bottom with the words "**Safeguards Information**"

See 10 CFR 73.22(f)



Transportation of SGI Documents

Outer envelope or wrapper addressed to the intended recipient, address of the sender, not contain any markings or indication that the envelope or wrapper contains SGI

Transported by commercial delivery company providing nation-wide overnight service with computer tracking features, US first class, registered, express, or certified mail, or by any individual authorized access

Within a facility

Transported using a single opaque envelope or wrapper

See 10 CFR 73.22(f)



Preparation and Marking of Documents

Marked "**Safeguards Information**" in a conspicuous manner on the top and bottom of each page to indicate the presence of protected information

First page of SGI Document also contains

- (i) the name, title, and organization of the individual authorized to make a SGI determination, and who determined the document contains SGI;
- (ii) the date the document was originated or the SGI determination made;
- (iii) an indication that unauthorized disclosure is subject to civil and criminal sanctions

See 10 CFR 73.22(d)




Preparation and Marking of Documents (continued)

Transmittal letters or memoranda which do not contain SGI are marked to indicate that attachments or enclosures contain SGI but that the transmittal document does not (e.g., "When separated from SGI enclosure(s), this document is decontrolled")

Each item of correspondence should clearly indicate which portions contain SGI and which portions do not; however, portion marking is only required for correspondence to and from the NRC

See 10 CFR 73



Removal from SGI Category

Removed from SGI category (decontrolled) only after a determination is made that the information no longer meets the SGI criteria

Authority to determine if a document/information can be removed from SGI category is exercised by the NRC, with the NRC approval, or in consultation with the individual (or organization) making original SGI determination

- Indicate name and organization of individual removing document from SGI category and date of removal
- Reasonable effort should be made to notify other persons who have the document in their possession, that the document has been downgraded

See 10 CFR 73.22(h)



Reproduction of Documents Containing SGI

Reproduced to the minimum extent necessary, consistent with a “need-to-know” without permission of the originator

Reproduction equipment must be evaluated to ensure that unauthorized persons cannot access the SGI through retained memory or network connectivity

See 10 CFR 73.22(e)



Destruction of Matter Containing SGI

Destroyed by means approved for classified information or by tearing into small pieces, burning, shredding or any other method that precludes reconstruction by means available to the public at large (piece sizes no wider than one quarter (1/4) inch composed of several pages or documents and thoroughly mixed would be considered completely destroyed)

See 10 CFR 73.22(i)



Use of Electronic Systems

Processed or produced on a “stand-alone” computer system. “Stand-alone” means a computer or computer system with which access is limited to individuals that are approved for access to SGI. The “stand-alone” computer may not be connected to a network that is accessible to individuals that are not approved for access to SGI

Removable media containing SGI must be labeled "**Safeguards Information**" and stored in approved security storage container

See 10 CFR 73.22(d) and 73.22(g)



Use of Electronic Systems

If SGI is produced on a typewriter, the ribbon must be removed and stored in the same manner as other SGI (i.e. marked and placed in an approved storage container)

SGI files may be transmitted over a network if the file is encrypted

- Encryption must take place on a “stand-alone” computer
- Encryption standard: (Federal Information Processing Standards (FIPS) 140-2 or later.)

See 10 CFR 73.22(f)



Telecommunications

Infrequent or non-repetitive telephone conversations regarding a physical security plan or program are permitted provided discussion is general in nature

Individuals should use care when discussing SGI at meetings or in the presence of others to ensure that SGI is not inadvertently released or compromised

SGI may only be transmitted over secure electronic devices that employ encryption approved by the NRC

See 10 CFR 73.22(f)



No Comment Policy

Occasionally, sensitive information appears in the public domain without authorization

Your response to questions raised about the accuracy, SGI designation, and/or technical merit of such information should be “no comment”



Questions?

Forward questions regarding SGI and its protection requirements to:

U.S. NRC

Office of Nuclear Security and Incident Response

Division of Security Operations

Information Security Branch

(301) 415-2278 or (301) 415-2214

