
INSPECTION PROCEDURE 75100 ATTACHMENT 06

PROTECTION OF SAFEGUARDS INFORMATION DURING CONSTRUCTION OF ADVANCED REACTORS

Effective Date: 10/20/2026

PROGRAM APPLICABILITY: IMC 2203

STRATEGIC PERFORMANCE AREA: SECURITY AND SAFEGUARDS

75100.06-01 INSPECTION OBJECTIVES

- 01.01 To determine whether the permit or license holder's information protection system effectively protects safeguards information (SGI), as defined in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.21 and 10 CFR 73.22 and prevents unauthorized disclosure.
- 01.02 To verify that the permit or license holder's physical protection program associated with this sample is designed and implemented to meet the general performance objective of 10 CFR 73.55(b).

75100.06-02 INSPECTION REQUIREMENTS

General Guidance

This inspection is conducted as a permit or license holder activates their SGI program in accordance with their security plan and NRC regulations. This IP is applicable to all advanced reactors under construction that are subject to oversight under the NRC's Advanced Reactor Construction Oversight Program (ARCOP). Verification through observation of activities may not be possible for all requirements. In such cases, the inspector(s) may review the appropriate permit or license holder's procedures and records.

Since advanced reactors will vary in design and licensing approaches, inspections will also be tailored to each site. The scope of inspections for advanced reactors will depend on the specific licensing framework and licensing basis selected by each permit or license holder. Therefore, some elements of this inspection procedure (IP) may be omitted. Additionally, many advanced reactors may be co-located with existing, operating reactors. Inspections of new reactors that use elements of existing site security plans do not need to include those elements that are the same as the operating reactors. For example, fitness-for-duty, access authorization, and safeguards information are areas where the NRC expects security plans to be essentially unchanged from the operating reactors' security plan.

Inspection activities are categorized into Tier I, II, or III based on their significance to the overall inspection program. Inspection activity tiers use a categorization process based on each program element's importance to overall physical security. Tier I elements have the highest

level of significance, while Tier III have the lowest level of significance. Typically, inspector(s) will inspect all Tier I and Tier II elements. Based on the inspection results of Tier I and II elements, or if time permits, the inspector(s) may inspect the Tier III elements.

Any inspection activities that do not align with the permit or license holder's licensing and design basis should not be inspected.

Specific Guidance

Inspector(s) should be familiar with the permit holder's or licensee's licensing basis, including its security plan. Other relevant documents may include site-specific and corporate implementing procedures, security post orders, and security program reviews and audits. Inspectors should pay particular attention to recent security plan changes that are relevant to the inspection activity.

The guidance in this procedure is provided as a tool which: (1) recommends to the inspector(s) certain methods and techniques for determining security program compliance; or (2) clarifies aspects of regulatory requirements associated with an inspection requirement. Completion of recommended actions contained in this guidance should not be viewed as mandatory and is only intended to assist the inspector(s).

The inspector(s) should coordinate the conduct of the inspection with the permit or license holder's staff before the inspection. Key areas of coordination are scheduling the dates and times to conduct, the observations of areas where SGI is stored, and requesting that the permit or license holder's SGI program procedures be made available for the inspector(s) to view.

The following types of non-public security-related information that is not classified as Restricted Data or National Security Information related to physical protection are considered SGI:

- a. The composite security plans for the facility or site.
- b. Site-specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical security system not easily discernible by members of the public.
- c. Alarm systems layouts showing the location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources for security equipment, and duress alarms not easily discernible by members of the public.
- d. Physical security orders and procedures issued by the permit or license holder for members of the security organization detailing:
 1. Duress codes;
 2. Patrol routes and schedules; or,
 3. Responses to security contingency events.
- e. Site-specific design features of plant security communication systems.
- f. Lock combinations, mechanical key design, or passwords integral to the physical security system.

- g. Documents and other matter that contain lists or locations of certain safety-related equipment explicitly identified in the documents or other matter as vital for purposes of physical protection, as contained in security plans, contingency measures, or plant-specific safeguards analyses.
- h. The composite safeguards contingency plan/measures for the facility or site.
- i. The composite facility officer training and qualification plan/measures disclosing features of the physical security system or response procedures.
- j. Information relating to on-site or off-site response forces, including size, armament of response forces, communications systems used for security purposes, and arrival times of such forces committed to respond to security contingency events.
- k. The adversary characteristics document and related information, including implementing guidance associated with the design basis threat in 10 CFR 73.1(a)(1) or 10 CFR 73.1(a)(2).
- l. Engineering and safety analyses, security-related procedures or scenarios, and other information revealing site-specific details of the facility or materials, if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security, by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material (SNM).
- m. Information related to the transportation of, or delivery to a carrier for transportation of a formula quantity of strategic special nuclear material or more than 100 grams of irradiated reactor fuel, including:
 - 1. The composite physical security plan for transportation;
 - 2. Schedules and itineraries for specific shipments of source material, byproduct material, high-level nuclear waste, or irradiated reactor fuel;
 - 3. Arrangements with and capabilities of local police response forces, and locations of safe havens identified along the transportation route;
 - 4. Limitations of communications during transport;
 - 5. Procedures for response to security contingency events;
 - 6. Information concerning the tactics and capabilities required to defend against attempted sabotage, or theft and diversion of SNM, irradiated reactor fuel, or related information; and,
 - 7. Engineering or safety analyses, security-related procedures or scenarios and other information related to the protection of the transported material if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or SNM.

- n. Information pertaining to safeguards and security inspections and reports, including portions of inspection reports, evaluations, audits, or investigations that contain:
 - 1. Details of a permit or license holder's physical security system; or
 - 2. Disclose uncorrected defects, weaknesses, or vulnerabilities in the system.
- o. Portions of correspondence that contain SGI as set forth in 10 CFR 73.22(a)(1) through 10 CFR 73.22(a)(3).

Tier I

02.01 Information Protection System

- a. **Verify that the permit or license holder, certificate holder, or applicant has established, implemented, and maintains an information protection system that includes the applicable measures for SGI as specified in 10 CFR 73.22 and subsequently published NRC Orders. (10 CFR 73.21(a)(1)(i) and 10 CFR 73.21(b)(2))**

Specific Guidance

Verify that the permit or license holder has developed a program to address the control, protection, and designation of SGI and that the implementing measures are documented in procedures.

02.02 Access to SGI

- a. **Verify that only authorized personnel are provided access to SGI and that the permit or license holder's process for authorizing access to SGI is based on the following criteria. (10 CFR 73.22(b)(1) and 10 CFR 73.22(b)(2))**

Personnel must have an established need-to-know. (10 CFR 73.22(b)(1))

Personnel must have a completed Federal Bureau of Investigation criminal history records check in accordance with 10 CFR 73.57 that is favorably adjudicated. (10 CFR 73.22(b)(1))

Personnel must be deemed trustworthy and reliable based upon a background check or other means approved by the Commission (10 CFR 73.22(b)(2)). The background check, at a minimum, must include:

- 1. **Verification of identity, based upon a fingerprint check;**
- 2. **Employment history;**
- 3. **Education; and**
- 4. **Personal references.**

Specific Guidance

Review the permit or license holder's implementing procedures for the control, protection, and designation of SGI to verify that the permit or license holder screens and provides access to SGI only to personnel who have met the requirements for access to SGI, in accordance with the regulations. The inspector(s) may request that the permit or license holder provide a listing of personnel who have been authorized access to SGI and query permit or license holder security management pertaining to the job description of those personnel who require continued access to SGI.

- b. Personnel must meet the exemption criteria of the category of individuals specified in 10 CFR 73.59 as exempt from the criminal history records check and background check requirements and have an established need-to-know. (10 CFR 73.22(b)(3))**

Specific Guidance

Refer to the guidance above.

02.03 Protection of SGI

- a. Verify that the permit or license holder stores unattended SGI in storage containers with locks that possess the characteristics identified in 10 CFR 73.2, Definitions, "Security Storage Containers" and "Locks." (10 CFR 73.22(c)(2))**

Specific Guidance

Request that the permit or license holder provide a tour of all areas that SGI is either stored, used, or developed to ensure that all areas have been provided a means to properly protect SGI that is unattended. Compare the security storage containers and locks that the permit or license holder uses for the protection of SGI to the criteria in 10 CFR 73.2, to ensure that the containers provide the required level of protection.

The definition of 'lock' in 10 CFR 73.2 is the following:

Lock, in the case of vaults or vault type rooms, means a three-position, manipulation resistant, dial type, built-in combination lock or combination padlock and, in the case of fences, walls, and buildings, means an integral door lock or padlock which provides protection equivalent to a six-tumbler cylinder lock. Lock, in the case of a vault or vault type room, also means any manipulation resistant, electromechanical device which provides the same function as a built-in combination lock or combination padlock, which can be operated remotely or by the reading or insertion of information, which can be uniquely characterized, and which allows operation of the device. Locked means protected by an operable lock.

The definition of 'security storage container' in 10 CFR 73.2 is the following:

Security storage container includes any of the following repositories:

1. For storage in a building located within a protected or controlled access area, steel filing cabinet equipped with a steel locking bar and a three-position, changeable combination, GSA approved padlock;
 2. A security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or interior plate, and is marked, General Services Administration Approved Security Container on the exterior of the top drawer or door;
 3. A bank safe-deposit box; and
 4. Other repositories which in the judgment of the NRC, would provide comparable physical protection.
- b. Verify that access to the combination to security storage containers, and keys to locks (if any), used to store SGI are controlled to preclude access to individuals not authorized access to SGI. (10 CFR 73.22(c)(2))**

Specific Guidance

Query the permit or license holder security management regarding the personnel who have access to the SGI security storage containers in each area to ensure that lock combinations, keys, etc., are provided only to those personnel designated for access to these storage containers to preclude unauthorized access to SGI. Not every individual authorized access to SGI should be provided access to security storage containers that contain SGI. Restricting access to security storage containers to only designated personnel reduces the potential for the compromise of SGI.

- c. Verify that the permit or license holder implements measures for the control of SGI while in use or outside of a locked security storage container and that the measures require SGI to remain under the control of an individual who is authorized access to SGI. (10 CFR 73.22(c)(1))**

Specific Guidance

Review the permit or license holder's implementing procedures for the control, protection, and designation of SGI to ensure the permit or license holder addresses the control of SGI when in use or located outside of a security storage container. Whenever possible, the inspector(s) should observe the implementation of these measures to verify that the implementation is consistent with the regulations and permit or license holder procedures. SGI within alarm stations or rooms continuously manned by authorized individuals need not be stored in a locked security storage container.

02.04 Processing, Reproducing, and Transmitting SGI

- a. Verify that the permit or license holder's stand-alone computers or computer systems used to process SGI are not connected to a network that is accessible by users not authorized access to SGI. (10 CFR 73.22(g)(1))**

Specific Guidance

Observe the computer systems that the permit or license holder uses for the development and processing of SGI. The inspector(s) should request that the permit or license holder demonstrate the isolation of these systems from accessible operational networks to verify that these systems and the information they possess are not accessible to unauthorized users.

- b. Verify that the permit or license holder's computers used to process SGI that are not located within an approved security storage container have a removable information storage medium that contains a bootable operating system (used to initialize the computer). (10 CFR 73.22(g)(2))**

Specific Guidance

Ensure that computers used to process SGI that are not located within an approved security storage container, have removable storage medium that contain bootable operating systems and software application programs. Data may be saved on the removable storage medium used to boot the operating system or a different removable storage medium.

- c. Verify that the permit or license holder locks removable storage mediums from SGI computers in a security storage container when not in use. (10 CFR 73.22(g)(2))**

Specific Guidance

No inspection guidance.

- d. Verify that equipment used by the permit or license holder to reproduce SGI does not allow unauthorized access to SGI by means of retained memory or network connectivity. (10 CFR 73.22(e))**

Specific Guidance

Review permit or license holder procedures for the reproduction or transmission of SGI utilizing technology such as copy machines or fax machines to ensure that the permit or license holder has established processes to protect the information such as memory purging and encryption. Request to observe the copy machines and fax machines used for SGI to verify that these machines are capable of the protection as stated in permit or license holder procedures and do not allow unauthorized access and reproduction.

- e. Verify that the permit or license holder's processes for transporting SGI outside of an authorized place of use or storage include the following measures: (1) documents are packaged in two sealed envelopes or wrappers to conceal the presence of SGI; (2) the inner envelope or wrapper contains the name and address of the intended recipient and is marked on both sides, top, and bottom with the words "SAFEGUARDS INFORMATION"; and (3) the outer envelope or wrapper is opaque, addressed to the recipient, contains the address of sender, bearing no markings or indication of the SGI contained within. (10 CFR 73.22(f)(1)).**

Specific Guidance

No inspection guidance.

Tier II

02.05 Protection of SGI

- a. **Verify that the permit or license holder reviews security-related information against the criteria for SGI and properly designates, protects, and controls SGI in accordance with regulations and site procedures. (10 CFR 73.21 and 10 CFR 73.22)**

Specific Guidance

Review the permit or license holder's implementing procedures for the control, protection, and designation of SGI to verify that the procedures address the review, screening, and evaluation of security-related information to ensure proper designation. Verify that these designation processes are conducted at each location that security-related information is processed or developed to ensure the proper protection of information designated SGI.

- b. **Verify that the permit or license holder's security storage containers used to store SGI do not bear identifying marks that indicate or identify the sensitivity of the information contained within. (10 CFR 73.22(c)(2))**

Specific Guidance

No inspection guidance.

02.06 Marking of SGI

- a. **Verify that the permit or license holder implements a process to ensure that documents or other matter, containing SGI, are conspicuously marked on the top and bottom of each page (e.g., "SAFEGUARDS INFORMATION"). (10 CFR 73.22(d)(1))**

Specific Guidance

No inspection guidance.

- b. **Verify that the permit or license holder's processes used to prepare documents containing SGI for delivery to the NRC include marking of transmittal letters or memoranda to indicate that attachments or enclosures contain SGI, but that the transmittal document or other matter does not (e.g., "Enclosure (or attachment) transmitted herewith contains Safeguards Information. When separated from Enclosure (or attachment), this transmittal document is decontrolled."). (10 CFR 73.22(d)(2))**

Specific Guidance

No inspection guidance.

02.07 Processing, Reproducing, and Transmitting SGI

- a. **Except under emergency or extraordinary conditions, verify that the permit or license holder's processes for the electronic transmission of SGI outside of an authorized place of use or storage include the use of NRC approved secure electronic devices, such as facsimiles or telephone devices or electronic mail that is encrypted by (Federal Information Processing Standard (FIPS) 140-2 or later) a method that has been approved by the NRC. (10 CFR 73.22(f)(3))**

Specific Guidance

Observe electronic devices used for the transmission, and preparation for transmission, of SGI to ensure that these devices either have the capability to encrypt and/or transmit SGI in accordance with regulatory requirements. Ensure the information is produced by a self-contained secure automated data processing system and transmitters and receivers implement the information handling processes that provide assurance that SGI is protected before and after transmission. Physical security events required to be reported under 10 CFR 73.1200 are considered to be extraordinary conditions.

02.08 Removal from SGI Category and SGI Destruction

- a. **Verify that the permit or license holder implements a process for the removal of documents or other matter from the SGI category when the information no longer meets the criteria of SGI. (10 CFR 73.22(h))**

Specific Guidance

Review recently decontrolled documents or other matter to ensure that they do not disclose SGI in another form or when combined with other unprotected information, do not disclose SGI.

- b. **Verify that the permit or license holder's processes for decontrolling SGI include measures to obtain the authority to remove the information from the SGI category through NRC approval or through consultation with the organization or individual who made the original SGI determination. (10 CFR 73.22(h))**

Specific Guidance

Review the permit or license holder's procedures for decontrolling SGI to ensure that they include a review by the appropriate entity (usually the agency, department, or personnel who made the original designation) before decontrolling the information.

- c. **Verify that the permit or license holder has established a process for the destruction of SGI and that its method of destruction precludes reconstruction by means available to the public at large. (10 CFR 73.22(i))**

Specific Guidance

Review permit or license holder procedures to verify that the permit or license holder has established measures for the destruction of SGI when the information is no longer needed and that the methodologies (e.g., burning, shredding, etc.) prevent reconstruction of the SGI media through any means of reconstruction available to the

public at large. Piece sizes no wider than one-quarter inch composed of several pages or documents thoroughly mixed are considered completely destroyed.

Tier III

02.09 Marking of SGI

- a. **Verify that the permit or license holder implements a process to ensure that the first page of documents containing SGI display: the name, title, and organization of the individual authorized to make an SGI determination; who has determined that the document or other matter contains SGI; the date the determination was made; and, indicates that unauthorized disclosure will be subject to civil and criminal sanctions. (10 CFR 73.22(d)(1))**

Specific Guidance

No inspection guidance.

- b. **Verify that the permit or license holder's processes used to prepare documents containing SGI for delivery to the NRC include portion marking, for the transmittal document, but not the attachment, in accordance with the regulation. (10 CFR 73.22(d)(3))**

Specific Guidance

No inspection guidance.

02.10 Reviews

Events and Logs. Review and evaluate the permit or license holder's physical security event log for events associated with the permit or license holders SGI program and follow-up, if appropriate, Review any written follow-up reports of physical security events associated with the permit or license holders SGI program. (10 CFR 73.55(b)(10), 10 CFR 73.1205, 10 CFR 73.1210))

Security Program Reviews. Verify that the permit or license holder is conducting security program reviews in accordance with 10 CFR 73.55(m) and that the permit or license holder's SGI program is included in the review, as required by regulation. (10 CFR 73.55(m))

Identification and Resolution of Problems. Verify that the permit or license holder is identifying issues related to the SGI program at an appropriate threshold and entering them in the permit or license holder's problem identification and resolution program. Verify that the permit or license holder has appropriately resolved the issues regarding regulatory requirements for a selected sample of problems associated with the SGI program. (10 CFR 73.55(b)(10))

Specific Guidance

Before the inspection, the inspector(s) should determine if a Security Event Report (SER), in accordance with 10 CFR 73.1205, has been submitted to the NRC by the

permit or license holder. Assess if additional follow-up under this IP is warranted for the conditions or corrective actions associated with the SER.

Review and evaluate permit or license holder physical security event log entries documented in accordance with 10 CFR 73.1210 that are associated with the SGI program. If discrepancies or deficiencies are identified during this review, the inspector(s) should follow-up, as necessary.

The inspector(s) should review the documented results of the security program reviews or audits performed by the permit or license holder to ensure the continued effectiveness of its SGI program. Ensure that the reviews have been conducted in accordance with the requirements of 10 CFR 73.55(m). Review the report(s) to identify any findings that were identified via the review or audit to ensure the findings were entered into the permit or license holder's corrective action program.

The inspector(s) should review a sample of entries in the permit or license holder's problem identification and resolution program associated with the SGI program. The intent of this review is to verify that the permit or license holder is identifying deficiencies at the appropriate threshold, tracking deficiencies for trending, and correcting deficiencies commensurate with their security significance.

71500.06-03 RESOURCE ESTIMATE

Approximately 4 hours of inspection effort are allocated for this IP. This estimate may vary depending on site-specific considerations.

71500.06-04 PROCEDURE COMPLETION

This IP is complete when sufficient inspection activities are performed to accomplish the IP objectives. Typically, this will include the available Tier I and Tier II elements. Consult with the Chief, Advanced Reactor Oversight Branch if needed to determine IP completion.

END

Attachment 1: Revision History for IP 75100.06

Revision History for IP 75100.06

Commitment Tracking Number	Accession No. Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession No. (Pre-Decisional, Non-Public Information)
N/A	ML26243A448 10/20/26 CN 26-048	Initial issuance.	N/A	N/A