INSPECTION PROCEDURE 81000.06

PROTECTION OF SAFEGUARDS INFORMATION

PROGRAM APPLICABILITY: IMC 2200, Appendix A

81000.06-01 INSPECTION OBJECTIVES

01.01 To determine if the licensee'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 licensee's physical protection program associated with this sample is designed and implemented to meet the general performance objective of 10 CFR 73.55(b).

81000.06-02 INSPECTION REQUIREMENTS

General Guidance.

This inspection procedure (IP) was developed to ensure the operational program established for implementation at a plant licensed in accordance with Title 10 CFR Part 50 and 10 CFR Part 52 meets all U.S. Nuclear Regulatory Commission (NRC) requirements and objectives for operational program readiness. Note that this inspection is conducted as licensees activate the operational program. Therefore, verification through observation of activities may not be possible. In such cases, the inspector(s) should review the appropriate licensee procedures and conduct inspections of all associated areas to ensure program compliance upon implementation.

Through verification of the inspection requirements within this inspection procedure (IP), inspector(s) shall ensure that the licensee's physical protection program associated with this sample is designed and implemented to meet the general performance objective of 10 CFR 73.55(b). In preparing to complete this procedure, the inspector(s) should familiarize themselves with relevant documentation which may include, but is not limited to, the licensee's security plans, site specific and/or corporate implementing procedures, security post orders, and security program reviews and audits. Specifically, the inspector(s) should apply additional attention to recent security plan changes that could be relevant to the inspection activity.

Inspector(s) are responsible for ensuring each sample in the IP is completed and evaluated to a level which provides assurance that licensees are meeting NRC regulatory requirements within the security program area being inspected.

The guidance within this procedure is being provided as a tool which: (1) recommends to inspectors certain methods and techniques for determining licensee security program

compliance and effectiveness related to an inspection requirement or; (2) clarifies certain aspects of a regulatory requirement associated with a particular inspection requirement. Where minimum sampling numbers are indicated (i.e., at least (three) intrusion detection system zones shall be tested, or at least 20 percent of the total personnel on a shift will be selected for weapons firing etc.), inspector(s) should adhere as closely as possible to the numbers identified in the guidance. Inspector(s) may expand the minimum number to aid in determining the extent of the condition, should compliance concerns arise. Completion of other recommended actions contained in this guidance should not be viewed as mandatory and is only intended to assist the inspector(s) in determining whether an inspection sample has been adequately addressed. Should questions arise regarding procedural requirements or guidance, the inspector(s) should consult with regional management or the Office of Nuclear Security and Incident Response (NSIR), the program office, for clarification.

The inspector(s) should coordinate the conduct of the inspection with the licensee's staff before the inspection. Key areas of coordination would be scheduling the dates and times to conduct, the observations of areas where SGI is stored, and requesting that the licensee'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 plan 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 system 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 licensee 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 communications 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, 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. Vehicle immobilization features, intrusion alarm devices, and communications systems;
4. Arrangements with and capabilities of local police response forces, and locations of safe havens identified along the transportation route;
5. Limitations of communications during transport;
6. Procedures for response to security contingency events;
7. Information concerning the tactics and capabilities required to defend against attempted sabotage, or theft and diversion of formula quantities of SNM, irradiated reactor fuel, or related information; and
8. 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:

1. Portions of 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; and
2. Reports of investigations containing general information may be released after corrective actions have been completed, unless withheld pursuant to other authorities, e.g., the Freedom of Information Act (5 U.S.C. 552).

o. Portions of correspondence that contain SGI as set forth in 10 CFR 73.22(a)(1) through 10 CFR 73.22(a)(3).

One hour has been allocated within the resource estimate of this IP for the inspector(s) to conduct physical protection program status verifications. The purpose of the status verification is to ensure that the implementation of the licensee's physical protection program is maintained in accordance with regulations, licensee security plans, and implementing procedures. The inspector(s) should conduct observations of physical protection program elements other than those inspected within this procedure.

02.01 Information Protection System.

Verify that the licensee, 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.

For the inspection of this requirement, the inspector(s) should verify that the licensee 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.

Verify that only authorized personnel are provided access to SGI and that the licensee's process for authorizing access to SGI is based on the following criteria. (10 CFR 73.22(b))

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

b. 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))

c. 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.

d. 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.

For the inspection of this requirement, the inspector(s) should review the licensee's implementing procedures for the control, protection, and designation of SGI to verify

that the licensee 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 licensee provide a listing of personnel who have been authorized access to SGI and query licensee security management pertaining to the job description of those personnel who require continued access to SGI.

02.03 Protection of SGI.

a. Verify that the licensee 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.

For the inspection of this requirement, the inspector(s) should request that the licensee 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. The inspector(s) should compare the security storage containers and locks that the licensee 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.

b. Verify that the combinations to security storage containers used to store SGI are controlled to preclude individuals not authorized access to SGI. (10 CFR 73.22(c)(2))

Specific Guidance.

For the inspection of this requirement, the inspector(s) should query licensee 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 licensee 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.

For the inspection of this requirement, the inspector(s) should review the licensee's implementing procedures for the control, protection, and designation of SGI to ensure the licensee 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 licensee 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 licensee'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.

For the inspection of this requirement, the inspector(s) should observe the computer systems that the licensee uses for the development and processing of SGI. The inspector(s) should request that the licensee 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 licensee'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.

For the inspection of this requirement, the inspector(s) should 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 licensee 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 licensee 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.

When inspecting this requirement, the inspector(s) should review licensee procedures for the reproduction or transmission of SGI utilizing technology such as copy machines or FAX machines to ensure that the licensee has established processes to protect the information such as memory purging and encryption. The inspector(s) should 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 licensee procedures and do not allow unauthorized access and reproduction.

e. Verify that the licensee'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.

02.05 Protection of SGI.

a. Verify that the licensee 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.

For the inspection of this requirement, the inspector(s) should review the licensee’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. The inspector(s) should also 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 licensee’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 licensee 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 licensee’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.

Except under emergency or extraordinary conditions, verify that the licensee'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.

For the inspection of this requirement, the inspector(s) should observe all the 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 73.71 are considered to be extraordinary conditions.

02.08 Removal from SGI Category and SGI Destruction.

a. Verify that the licensee 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.

For the inspection of this requirement, inspector(s) should 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 licensee'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.

For the inspection of this requirement the inspector(s) should review the licensee'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 licensee 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.

For the inspection of this requirement, the inspector(s) should review licensee procedures to verify that the licensee 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.

02.09 Marking of SGI.

a. Verify that the licensee implements a process to ensure that the first page of documents containing SGI bear 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 licensee'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 licensee event reports, safeguards log entries, and corrective action program entries for the previous 12 months (or since the last inspection) that concern the protection of SGI program, and follow up, if appropriate.

Security Program Reviews. Verify that the licensee is conducting security program reviews in accordance with 10 CFR 73.55(m) and that the licensee's SGI program was included in a review as required by the regulation. (10 CFR 73.55(m))

Problem Identification and Resolution. Verify that the licensee identifies problems with the SGI program at an appropriate threshold and enters the problems in the corrective action program. Verify that the licensee has appropriately resolved the regulatory requirement issue for a selected sample of problems with protection of SGI.

If applicable, see IP 71152, "Problem Identification and Resolution," for additional guidance. (10 CFR 73.55(b)(10))

Specific Guidance.

The inspector(s) should review safeguards log entries, licensee condition reports, licensee corrective action program entries, etc., for the previous 12 months to determine whether the licensee has experienced issues with the implementation of its SGI program. The inspector(s) should follow-up on issues identified to ensure the licensee has taken appropriate corrective actions to prevent a re-occurrence of the issues identified. For the inspection of this requirement the inspector(s) should review the documented results of the security program reviews or audits performed by the licensee to ensure the continued effectiveness of its SGI program. The inspector(s) should ensure that the reviews have been conducted in accordance with the requirements of 10 CFR 73.55(m). The inspector(s) should also request that the licensee provide a copy of the report that was developed and provided to licensee management for review. The inspector(s) should review the report to identify any findings that were identified via the review or audit to ensure the findings were entered in the licensee's corrective action program.

81000.06-03 RESOURCE ESTIMATE

The resource estimate for this IP is approximately 10 hours of direct on-site inspection. The sample size for this procedure is 24.

81000.06-04 REFERENCES

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

10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants"

10 CFR Part 73, "Physical Protection of Plants and Materials"

5 U.S.C. 552, "The Freedom of Information Act"

IP 71152, "Problem Identification and Resolution"

END

Attachment 1: Revision History for IP 81000.06, "Protection of Safeguards Information"

Attachment 1 - Revision History for IP 81000.06, “Protection of Safeguards Information”

Commitment Tracking Number	Accession Number 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	ML18324A829 02/13/19 CN 19-007	Initial issuance of IP to support operational program inspections described in IMC 2200, “Security Inspection Program for Construction.”	N/A	ML18324A827