INSPECTION PROCEDURE 81607

PROTECTION OF SAFEGUARDS INFORMATION AND SAFEGUARDS INFORMATION MODIFIED HANDLING – NON-POWER REACTORS

Effective Date: 06/01/2020

PROGRAM APPLICABILITY: IMC 2545

81607-01 INSPECTION OBJECTIVE

The objective of this inspection procedure (IP) is to gather information to determine whether reasonable assurance exists that licensee activities, since the last inspection, were conducted in accordance with regulatory requirements in Title 10 of the *Code of Federal Regulations* (CFR) Part 73, "Physical Protection of Plants and Materials."

01.01 Safeguards Information. To assure that the licensee has established, implemented and maintained an information protection system that protects Safeguards Information (SGI) against unauthorized disclosure. [10 CFR 73.21(a)(i), 10 CFR 73.21(a)(iii)]

01.02 Safeguards Information–Modified Handling. To assure that the licensee has established, implemented and maintained an information protection system that protects Safeguards Information–Modified Handling (SGI-M) against unauthorized disclosure. [10 CFR 73.21(a)(ii)]

01.03 Access Authorization. To assure that the licensee has an access authorization program that will provide a basis upon which to make a determination of trustworthiness and reliability of personnel granted access to SGI or SGI-M.

81607-02 INSPECTION REQUIREMENTS

02.01 Safeguards Information. Verification of the protection of SGI in the hands of any person and, in part, related to: 1) a formula quantity of strategic special nuclear material (SNM); or, 2) transportation of or delivery to a carrier for transportation of more than 100 grams of irradiated reactor fuel. [10 CFR 73.22]

a. Information to be protected. Verify that the licensee is protecting the types of information and documentation that is considered as SGI, including: fixed site physical protection; in transit physical protection; inspections, audits, and evaluations; correspondence; and other information as determined by the Commission. [10 CFR 73.22(a)(1)-(a)(5)]

b. Conditions for access.

1. Verify that the licensee ensures personnel have an established “need to know”. [10 CFR 73.22(b)(1)]

2. Verify that the licensee ensures personnel have completed a Federal Bureau of Investigation fingerprint-based criminal history records check. [10 CFR 73.22(b)(1), 10 CFR 73.57]

3. Verify that the licensee ensures a determination of trustworthiness and reliability based upon a background check or other means approved by the commission. [10 CFR 73.22(b)(2)]

4. As applicable, verify that the licensee appropriately determines personnel meet the exemption criteria of the category of individuals to be exempt from the criminal history records check and background check. The licensee must still ensure exempt personnel have an established “need to know”. [10 CFR 73.22(b)(3), 10 CFR 73.59]

c. Protection while in use or storage.

1. Verify that the licensee ensures SGI is constantly attended by authorized personnel while in use or not in storage. [10 CFR 73.22(c)(1)]

2. Verify that the licensee stores unattended SGI in locked security storage containers that do not bear identifying marks indicating or identifying the sensitivity of the information contained within. [10 CFR 73.2, 10 CFR 73.22(c)(2)]

3. Verify that the licensee controls access to the combination for security storage containers, used to store SGI, to preclude access to individuals not authorized access to SGI. [10 CFR 73.22(c)(2)]

d. Preparation and marking.

1. 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, i.e., “Safeguards Information.” [10 CFR 73.22 (d)(1)]

2. 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, and 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)]

3. Verify that the licensee implements a process to prepare documents or other matter containing SGI for delivery to the NRC that includes marking of transmittal letters or memoranda to indicate that attachments or enclosures contain SGI but that the transmittal document or other matter does not (i.e., “when separated from SGI attachment or enclosure, this document is decontrolled.”). [10 CFR 73.22(d)(2)]

4. As applicable, verify that the licensee implements a process to prepare documents containing SGI for delivery to the NRC that includes portion marking for the transmittal document, but not the attachment. [10 CFR 73.22(d)(3)]

e. Reproduction. 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)]

f. Transmission.

1. Verify that the licensee implements a process for transmission of SGI outside of an authorized place of use or storage that includes 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 and contains the address of both sender and recipient, while bearing no markings or indication of the SGI contained within. [10 CFR 73.22(f)(1)]

2. Except under emergency or extraordinary conditions, verify that the licensee implements a process for the electronic transmission of SGI outside of an authorized place of use or storage that includes the use of NRC approved secure electronic devices, such as facsimiles or telephone devices or electronic mail that is encrypted (i.e., Federal Information Processing Standard (FIPS) 140-2 or later) by a method that has been approved by the NRC. [10 CFR 73.22(f)(3)]

g. Processing.

1. Verify that the licensee processes SGI using stand-alone computers, laptop computers, or computer systems that are not connected to a network or otherwise accessible by users not authorized access to SGI. [10 CFR 73.22(g)(1), 10 CFR 73.22(g)(3)]

2. Verify that 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. [10 CFR 73.22(g)(2)]

3. Verify that the licensee locks removable storage media from SGI computers in a security storage container when not in use. [10 CFR 73.22(g)(2)]

4. Verify that laptop computers used to process SGI are located within an approved and lockable security storage container. [10 CFR 73.22(g)(2), 10 CFR 73.22(g)(3)]

h. Removal from SGI Category.

1. 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)]

2. Verify that the process for decontrolling SGI includes 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 determination. [10 CFR 73.22(h)]

i. Destruction of SGI. 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)]

02.02 Safeguards Information–Modified Handling. Verification of the protection of SGI-M in the hands of any person and related to: 1) non-power reactors that possess SNM of moderate strategic significance; or, 2) non-power reactors that possess SNM of low strategic significance. [10 CFR 73.23]

a. Information to be protected. Verify that the licensee is protecting the types of information and documentation that is considered as SGI-M, including: fixed site physical protection; in transit physical protection; inspections, audits, and evaluations; correspondence; and other information as determined by the Commission. [10 CFR 73.23(a)(1)-(a)(5)]

b. Conditions for access.

1. Verify that the licensee ensures personnel have an established “need to know”. [10 CFR 73.23(b)(1)]

2. Verify that the licensee ensures personnel have completed a Federal Bureau of Investigation fingerprint-based criminal history records check. [10 CFR 73.23(b)(1), 10 CFR 73.57]

3. Verify that the licensee ensures a determination of trustworthiness and reliability based upon a background check or other means approved by the commission. [10 CFR 73.23(b)(2)]

4. As applicable, verify that the licensee appropriately determines personnel meet the exemption criteria of the category of individuals to be exempt from the criminal history records check and background check. The licensee must still ensure exempt personnel have an established “need to know”. [10 CFR 73.23(b)(3), 10 CFR 73.59]

c. Protection while in use or storage.

1. Verify that the licensee ensures SGI-M is constantly attended by authorized personnel while in use or not in storage. [10 CFR 73.23(c)(1)]

2. Verify that the licensee stores unattended SGI-M in locked file drawers or cabinets that do not bear identifying marks indicating or identifying the sensitivity of the information contained within. [10 CFR 73.2, 10 CFR 73.23(c)(2)]

3. Verify that the licensee controls access to the combination for the containers, used to store SGI, to preclude access to individuals not authorized access to SGI-M. [10 CFR 73.23(c)(2)]

d. Preparation and marking.

1. Verify that the licensee implements a process to ensure that documents or other matter, containing SGI-M, are conspicuously marked on the top and bottom of each page, i.e., “Safeguards Information–Modified Handling.” [10 CFR 73.23(d)(1)]

2. Verify that the licensee implements a process to ensure that the first page of documents containing SGI-M bear the name, title, and organization of the individual authorized to make an SGI-M determination, and who has determined that the document or other matter contains SGI-M; the date the determination was made; and indicates that unauthorized disclosure will be subject to civil and criminal sanctions. [10 CFR 73.23(d)(1)]

3. Verify that the licensee implements a process to prepare documents or other matter containing SGI-M for delivery to the NRC that includes marking of transmittal letters or memoranda to indicate that attachments or enclosures contain SGI-M but that the transmittal document or other matter does not (i.e., “when separated from Safeguards Information designated as Safeguards Information–Modified Handling enclosure(s), this document is decontrolled.”). [10 CFR 73.23(d)(2)]

4. As applicable, verify that the licensee implements a process to prepare documents containing SGI-M for delivery to the NRC that includes portion marking for the transmittal document, but not the attachment. [10 CFR 73.23(d)(3)]

e. Reproduction. Verify that equipment used by the licensee to reproduce SGI-M does not allow unauthorized access to SGI-M by means of retained memory or network connectivity. [10 CFR 73.23(e)]

f. Transmission.

1. Verify that the licensee implements a process for transmission of SGI-M outside of an authorized place of use or storage that includes the following measures: (1) documents are packaged in two sealed envelopes or wrappers to conceal the presence of SGI-M; (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–Modified Handling"; and (3) the outer envelope or wrapper is opaque and contains the address of both sender and recipient, while bearing no markings or indication of the SGI-M contained within. [10 CFR 73.23(f)(1)]

2. Except under emergency or extraordinary conditions, verify that the licensee implements a process for the electronic transmission of SGI-M outside of an authorized place of use or storage that includes the use of NRC approved secure electronic devices, such as facsimiles or telephone devices or electronic mail that is encrypted (i.e., FIPS 140-2 or later) by a method that has been approved by the NRC. [10 CFR 73.23(f)(3)]

g. Processing.

1. Verify that the licensee processes SGI-M using stand-alone computers, laptop computers, or computer systems that are assigned to the licensee's or contractor's facility. [10 CFR 73.23(g)(1), 10 CFR 73.23(g)(3)]

2. Verify that the licensee protects electronic files containing SGI-M, either by password or encryption, to prevent unauthorized individuals from gaining access. [10 CFR 73.23(g)(1)]

3. Verify that, if the licensee transmits files over a network, the files are encrypted using a method that has been validated by NIST to conform to FIPS 140-2 or later. [10 CFR 73.23(g)(2)]

4. Verify that the licensee saves files containing SGI-M to removable media and stores in locked file drawers or cabinets. [10 CFR 73.23(g)(2)]

5. Verify that laptop computers used to process SGI-M are located within locked file drawers or cabinets. [10 CFR 73.23(g)(3)]

h. Removal from SGI Category.

1. 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-M. [10 CFR 73.23(h)]

2. Verify that the process for decontrolling SGI includes 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 determination. [10 CFR 73.23(h)]

i. Destruction of SGI. 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 73.23(i)]

02.03 Access Authorization.

a. Criminal History Records Check. Verify that the licensee meets the requirements regarding fingerprinting individuals who are seeking or permitted access to SGI or SGI-M.

1. Verify that the licensee is appropriately basing final determinations utilizing information received from the FBI. [10 CFR 73.57(c), EA-06-203]

2. Verify that the licensee has a process for allowing individuals the right to complete and correct information. [10 CFR 73.57(e), EA-06-203]

3. Verify that the licensee appropriately protects records and personal information from unauthorized disclosure. [10 CFR 73.57(f), EA-06-203]

4. Verify that the licensee obtains fingerprints for a criminal history records check for each individual who is seeking or permitted access to SGI or SGI-M. [10 CFR 73.57(a)(2), 10 CFR 73.57(b)(1), EA-06-203]

b. NRC-Approved Reviewing Official. Verify that the licensee has an NRC-approved reviewing official who provides determinations that individuals are trustworthy and reliable based on the results of an FBI fingerprint-based criminal history records check. [EA-06-203]

81607-03 INSPECTION GUIDANCE

This section is intended to provide guidance to assist the inspector in measuring the licensee's performance in each of the preceding sections. The statements below do not represent regulatory requirements, but are standards and methods by which the individual elements may be judged.

The licensee is required to have developed and implemented a program, procedures, or processes to address the control, protection and designation of SGI or SGI-M. The process should address the review, screening and evaluation of security-related information to ensure proper designation and the appropriate level of protection. Based on documents and records reviewed during the course of the inspection, the inspector should be able to verify that information has been designated and protected appropriately.

The following types of information are examples of what can be considered SGI or SGI-M: physical security plan and implementing procedures; site specific drawings, sketches, diagrams, and maps; details of security alarm and communication systems; lock combinations, mechanical key design, and passwords; information which identifies certain equipment or areas as vital; response plans, patrol routes, and duress codes; description of size, armament, or disposition of onsite and offsite security and response forces; engineering or safety analyses related to security features; uncorrected or unmitigated defects, weaknesses, or vulnerabilities; and any associated correspondence containing SGI or SGI-M.

The following types of information are examples of what can be considered SGI: safeguards contingency plan; transportation security plan; schedules and itineraries for shipments; vehicle immobilization features, alarms, and communication systems; arrangements with and capabilities of law enforcement agencies and response forces; locations of safe havens along the route; limitations of communications during transport; response procedures during shipment; and engineering or safety analyses related to transportation.

Licensees are required to include a fingerprint-based FBI criminal history records check as part of the background screening conducted for individuals who are seeking or permitted access to SGI or SGI-M. The inspector should note that there may be some overlap with the access authorization program or process in place for unescorted access to vital areas or unescorted access to SNM. Prior to being granted access, an individual must be determined to be trustworthy and reliable based on the results of a background check and FBI fingerprint-based criminal history records check. Determinations should look at recent results and may not be based solely on arrests more than 1 year old with no information on disposition of the case or for arrests resulting in a dismissal of the charge or an acquittal. The inspector should review whether the licensee has made any final adverse determinations and if the individual was permitted to correct and complete information obtained during the criminal history records

check. The inspector should confirm that the licensee has a system to protect the records and personal information from unauthorized disclosure. Records review should indicate that fingerprint and criminal history records from the FBI are retained until at least one year following termination of an individual's unescorted access. Relief from fingerprinting and criminal history records checks are afforded to those categories of individuals listed in 10 CFR 73.59. The inspector may consider requesting an updated listing of licensee personnel who have been authorized access to SGI. Facilities with one or two staff members may find generating these types of lists to be an unnecessary burden. Alternatively, a sample of records related to fingerprinting results or trustworthiness and reliability determinations contained in personnel files should suffice.

Licensees are required to have at least one current documented NRC-approved reviewing official who has access to Safeguards Information at the facility. The inspector should review processes and records to verify that the NRC-approved reviewing official has the required FBI fingerprint based criminal history records before granting access to SGI or SGI-M persons desiring such access. Records review should also indicate that the NRC-approved reviewing official is basing a trustworthiness and reliability determination on the results from the FBI fingerprint-based criminal history records check. The NRC-approved reviewing official may or may not be the same person that makes a final determination on whether or not to grant an individual access.

During a tour of the facility and while obtaining documents or records for review, the inspector should observe the locations where SGI or SGI-M is used and stored. The inspector may choose to review procedures or interview personnel to determine who has knowledge of lock combinations and access to the storage locations. Typically, licensed operators will have some knowledge of security-related information, but may not have access to all types of information protected at the facility. Based on this, licensees may decide to designate a smaller subset of individuals (i.e. facility management) to have the ability to open storage locations.

SGI: While unattended, SGI must be stored in a locked security storage container (e.g. security filing cabinet externally marked "General Services Administration [(GSA)] Approved Security Container"; steel filing cabinet equipped with a steel locking bar and a three position, changeable combination, GSA-approved padlock).

SGI-M: While unattended, SGI-M must be stored in a locked file drawer or cabinet.

The licensee is required to mark all documents or other matter containing SGI or SGI-M. During document and records review, the inspector should observe the presence of markings and determine whether the licensee has appropriately marked the documents or other matter in accordance with the regulations or regulatory guidance (i.e. RG 5.79, "Protection of Safeguards Information").

The licensee is required to establish processes to protect SGI and SGI-M when utilizing technology such as copy machines for reproduction (i.e. memory purging). The inspector should request to observe all of the electronic devices used for reproduction of SGI to verify that these machines are capable of the protection required and do not allow unauthorized access and reproduction.

The licensee is required to establish processes to protect SGI and SGI-M when utilizing technology such as FAX machines for transmission (i.e. encryption). The inspector should request to observe all of the electronic devices used for the transmission, and the preparation

for transmission, of SGI or SGI-M to ensure that these devices either have the capability to encrypt and/or transmit SGI or SGI-M in accordance with regulatory requirements. Physical security events required to be reported under 10 CFR 73.71 are considered to be extraordinary conditions.

For the inspection of this requirement, the inspector(s) should observe the use and storage of computer systems and removable media that the licensee uses for the storage, processing, and production of SGI and SGI-M.

SGI: The inspector should request that the licensee demonstrate the isolation of the stand-alone systems from accessible operational networks to verify that these systems and the information they possess are not accessible to unauthorized users. The inspector 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.

SGI-M: The inspectors should confirm that the systems used for the storage, processing, and production of SGI-M are assigned to the licensee. The inspector should request that the licensee demonstrate the encryption or password protection in place for files containing SGI-M. The inspector should verify that files containing SGI-M are stored on removable media and stored in a locked file drawer or cabinet.

The inspector should review recently decontrolled documents or other matter to ensure that they do not disclose SGI or SGI-M in another form or when combined with other unprotected information (i.e., the aggregate of multiple sources of information). The inspector should review the process for decontrolling SGI or SGI-M to ensure that it includes a review and approval by the appropriate entity (usually the agency, department, or personnel who made the original designation) before decontrolling the information. Information previously designated as SGI or SGI-M by the NRC staff would require communication, review, and approval by the NRC staff before changing or removing the designation.

The inspector should verify that the licensee has an established process for the destruction of SGI or SGI-M when the information is no longer needed and that the methodologies (e.g., burning or shredding) prevent reconstruction of the SGI media through any means of reconstruction available to the public at large. Shredded pieces no wider than one quarter inch, composed of several pages of documents thoroughly mixed, are considered completely destroyed.

81607-04 RESOURCE ESTIMATE

For planning purposes, the estimated, direct, onsite inspection effort to complete this inspection procedure is 4 hours. Actual inspection at any facility may require more or less effort depending on past inspection history, changes since the last inspection, conditions at the facility, and significance of the inspection findings.

81607-05 PROCEDURE COMPLETION

The inspection of each of the applicable areas described above will constitute completion of this procedure. The frequency at which this inspection procedure is to be completed is dependent on the quantity of SNM possessed and is described in Manual Chapter 2545. The typical frequencies are biennially for facilities possessing SNM MSS or triennially for facilities possessing SNM LSS.

81607-06 REFERENCES

U.S. NRC Designation Guide for Safeguards Information, DG-SGI-1

Manual Chapter 2545, “Research and Test Reactor Inspection Program”

RG 5.79, “Protection of Safeguards Information”

EA-06-203, “Issuance of Order Imposing Fingerprinting and Criminal History Records Check Requirements for Access to Safeguards Information”

END

Attachment:
1. Revision History Sheet for IP 81607

Attachment 1 - Revision History for IP 81607

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 Number (Pre-Decisional, Non-Public Information)
	ML19190A271 03/13/20 CN 20-015	Initial issue to support inspection of research and test reactor programs described in IMC 2545.	None	ML19205A354