INSPECTION PROCEDURE 81811

PROTECTION OF SAFEGUARDS INFORMATION BY DESIGN CERTIFICATION APPLICANTS AND VENDORS

PROGRAM APPLICABILITY: IMC 2507, IMC 2508

81811-01 INSPECTION OBJECTIVES

To determine if the design applicant and vendor entities authorized to hold Safeguards information have enacted an information protection system that effectively protects Safeguards Information (SGI), as defined in Title 10 of *the Code of Federal Regulations* (CFR) 73.21, and 10 CFR 73.22, and the system prevents unauthorized disclosure. This is inclusive of control of SGI information provided by the NRC to applicants and vendors, as well as information developed by the applicant or vendor, for example, when the NRC forcing function is provided and then used to develop a design specific aircraft impact assessment.

81811-02 INSPECTION REQUIREMENTS

In preparing to complete this procedure, the inspector(s) should familiarize themselves with relevant documentation which may include, but is not limited to, the SGI program and/or corporate implementing procedures, reviews and audits. The inspector(s) should review past SGI program inspection reports for the facility and any Commission Orders specific to that facility directing protections for Safeguards information. During this review the inspector should consider previously inspected requirements to ensure all requirements are being inspected regularly.

Inspector(s) are responsible for completing the inspection procedure in order to support an evaluation of design applicant's or vendor's ability to meet the U.S. Nuclear Regulatory Commission (NRC) requirements for the security program area being inspected.

This guidance is being provided as a tool which: (1) recommends to inspectors certain methods and techniques for determining compliance by NRC authorized design and vendor entities with security program requirements and; (2) clarifies certain aspects of a regulatory requirements associated with particular inspection requirements. Completion of other recommended actions contained in this guidance must not be viewed as mandatory, for an inspector to determine whether an inspection aspect has been adequately addressed. Should questions arise regarding procedural requirements or guidance, the inspector(s) should consult with the Office of Nuclear Reactor Regulation (NRR), Division of Reactor Oversite (DRO) or the Office of Nuclear Security and Incident Response (NSIR), for clarification.

If the inspection is announced, the lead inspector should coordinate with the staff of the NRC authorized entity. 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 SGI program procedures be made available for the inspection team to review.

The following types of non-public security-related information, which 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 member of the public.

d. Site-specific design features of plant security communication systems.

e. Lock combinations, mechanical key design, or passwords integral to the physical security system.

f. Documents and other matter that contain lists or locations of certain safety-related equipment explicitly identified in the document or other matter as vital for purposes of physical protection, as contained in plant-specific safeguards analyses.

g. Information that reflects the characteristics and attributes of the design basis threat of radiological sabotage.

h. Engineering and safety analyses, and other information revealing site-specific details of the facility or materials if the unauthorized disclosure of such analyses, 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, byproducts, or special nuclear material.

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

02.01 Information Protection System.

The NRC authorized entity shall establish, implement, and maintain 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 73.21(b)(2))

02.02 Access to SGI.

The NRC authorized entity shall permit only authorized personnel access to SGI and the 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 being exempt from the criminal history records and background check requirements and have an established need to know. (10 CFR 73.22(b)(3))

02.03 Protection of SGI.

a. The NRC authorized entity shall store 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))

b. Combinations to security storage containers, used to store SGI, is controlled to preclude access to individuals not authorized access to SGI.
(10 CFR 73.22(c)(2))

c. NRC authorized entity implements measures for the control of SGI while in use 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))

02.04 Processing, Reproducing, and Transmitting SGI.

a. NRC authorized entity's computers, computer systems and, networks 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))

b. NRC authorized entity'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))

c. The NRC authorized entity shall secure removable storage mediums from SGI computers in a security storage container when not in use. (10 CFR 73.22(g)(2))

d. Equipment used by the NRC authorized entity to reproduce SGI does not allow unauthorized access to the SGI by means of retained memory or network connectivity.
(10 CFR 73.22(e))

e. NRC authorized entity's processes for transporting SGI outside of an authorized place of use or storage shall 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)).

02.05 Protection of SGI.

a. The NRC authorized entity shall review security-related information against the criteria for SGI and properly designates, protects, and controls SGI in accordance with NRC regulations and site procedures. (10 CFR 73.21 & .22)

b. Verify that the NRC authorized entity's security storage containers used to store SGI shall not bear identifying marks that indicate or identify the sensitivity of the information contained within. (10 CFR 73.22(c) (2))

02.06 Marking of SGI.

a. The NRC authorized entity shall implement 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))

b. NRC authorized entity'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 (i.e., "when separated from SGI attachment or enclosure, this document is decontrolled.") (10 CFR 73.22(d)(2))

02.07 Processing, Reproducing, and Transmitting SGI.

The processes for the electronic transmission of SGI outside of an authorized place of use or storage shall include the use of NRC approved secure electronic devices, such as facsimiles or telephone devices or electronic mail that is encrypted by an NRC approved method, such as Federal Information Processing Standard (FIPS) 140-2 or later (unless under extraordinary conditions.) (10 CFR 73.22(f)(3))

2.08 Removal from SGI Category and SGI Destruction.

a. NRC authorized entity has a specific and controlled process for 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))

b. The processes for decontrolling SGI shall 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))

c. The process for the destruction of SGI and, the method of destruction, shall preclude reconstruction by means available to the public at large. (10 CFR 73.22(i))

02.09 Reviews.

Events and Logs. The NRC authorized entity shall maintain 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 shall follow up and maintain records of those actions.

Safeguard Information Program Reviews. The NRC authorized entity shall conduct reviews of their SGI program.

Problem Identification and Resolution of Problems. The NRC authorized entity shall identify problems with the protection of SGI program and enters the problems into the corrective action program, as appropriate for SGI topics. Identified problems shall be resolve while maintaining compliance with the regulatory requirements for the issue.

02.10 Marking of SGI.

a. The NRC authorized entity shall implement a process to ensure 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))

b. NRC authorized entity'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))

81811-03 INSPECTION GUIDANCE

Inspectors should verify by directly observing the process, either actual or demonstration/simulation to the maximum extent possible. Reviewing procedures alone should be accepted when demonstration or observation is not possible

03.01 Information Protection System.

For the inspection of this requirement, the inspector should verify that the NRC authorized entity or vendor has developed a program to address the control, protection and designation of SGI and that the implementing measures are documented in procedures.

03.02 Access to SGI.

The inspector should review the implementing procedures for the control, protection, and designation of SGI to verify that the NRC authorized entity or vendor 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 may request that the NRC authorized entity or

vendor provide a listing of personnel who have been authorized access to SGI and query the NRC authorized entity or vendor's security management pertaining to the job description of these personnel which requires that they maintain access to SGI.

03.03 Protection of SGI.

a. For the inspection of this requirement, the inspector(s) should tour of all areas in which 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 should compare the security storage containers and locks that the NRC authorized entity or vendor 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. For the inspection of this requirement, the inspector should query NRC authorized entity or vendor's security management regarding the personnel who have access to the SGI security storage containers. The inspector should verify that only those personnel designated for access to these storage containers have access to the key, the combination, etc. so as to preclude unauthorized access to SGI. Not every individual authorized access to SGI needs access to the security storage containers that contain SGI. Restricting access to security storage containers to only designated personnel reduces the potential for compromise of SGI.

c. The inspector should review the implementing procedures for the control, protection and designation of SGI to ensure the SGI is controlled and protected when in use. Whenever possible, the inspector should observe the implementation of these measures to verify that the implementation is consistent with NRC regulations and the NRC authorized entity's or vendor's procedures. SGI within alarm stations or rooms continuously manned by authorized individuals need not be stored in a locked security storage container.

03.04 Processing, Reproducing, and Transmitting SGI.

a. The inspector should observe the computer systems used for the development and processing of SGI. The inspector(s) should request that the NRC authorized entity or vendor 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. The inspector should ensure that computers used to process SGI, 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. No inspection guidance.

d. The inspector should review the procedures for the reproduction or transmission of SGI utilizing technology such as copy machines or FAX machines to ensure that the processes protect the information by such methods as memory purging and encryption. The inspector should request to observe the copy machines and FAX machines used for SGI to verify that these machines are capable of the protection stated in the

procedures and do not allow unauthorized access and reproduction.

e. No inspection guidance.

03.05 Protection of SGI.

a. For the inspection of this requirement, the inspector(s) should review the NRC authorized entities 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. No specific guidance

03.06 Marking of SGI.

Documents need not be designated and marked as SGI, top and bottom, if they are already marked and protected as classified information. Portions of the document (paragraphs, tables, charts, figures, etc.) containing SGI however must be properly marked to indicate the designation of the information contained therein.

03.07 Processing, Reproducing, and Transmitting SGI.

The inspector should observe all of 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. 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.

03.08 Removal from SGI Category and SGI Destruction.

a. The inspector 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. The inspector should review the 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. The inspector should review procedures to verify that measures for the destruction of SGI when the information is no longer needed are present, and the methodologies (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.

03.09 Reviews.

a.-c. Events and Logs, Safeguard Information Program Reviews, Problem Identification and Resolution.

The inspector should review safeguards log entries, condition reports, corrective action program entries, etc., for the previous 12 months to determine issues with the implementation of its SGI program. The inspector should follow-up on issues identified to ensure the appropriate corrective actions to prevent a re-occurrence of the issues identified are in-place or being implemented. The inspector should review the documented results of the security program reviews or audits performed to ensure the continued effectiveness of its SGI program.

03.10 Marking of SGI.

a. No inspection guidance.

b. Documents already designated, marked, and protected as classified information need not be marked as SGI, top and bottom. Portions of the document containing SGI must be properly marked to indicate the designation of the information contained.

81811-04 RESOURCE ESTIMATE

The resource estimate is approximately 6 hours of direct inspection effort, 12 hours of preparation, and 12 hours of documentation.

81811-05 PROCEDURE COMPLETION

Inspector(s) should attempt to ensure that each requirement identified in the inspection procedure is completed at each inspection. The inspection should be completed no less than triennially.

Documenting Inspection Results.

Inspection reports document issues identified during the inspection and will be developed in accordance with the requirements in IMC 0617, “Vendor and Quality Assurance Implementation Inspection Reports.”

81811-06 REFERENCES

Title 10 of *the Code of Federal Regulations* (10 CFR) 73.21, and 10 CFR 73.22

IMC 0617, “Vendor and Quality Assurance Implementation Inspection Reports.”

IMC 2507, “Vendor Inspections.”

IMC 2508, “Construction Inspection Program: Design Certification.”

END

Attachment 1: Revision History for IP 81811

Attachment 1 - Revision History for IP 81811

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)
N/A	ML16126A125 09/06/16 CN 16-022	Initial issuance. Completed four-year search for commitments and found none.	None	ML16126A121
N/A	ML20084G483 04/08/20 CN 20-020	Revised to align with organizational changes, format changes, and improve clarity.	None	None