INSPECTION PROCEDURE 81811

PROTECTION OF SAFEGUARDS INFORMATION BY DESIGN CERTIFICATION APPLICANTS AND VENDORS

PROGRAM APPLICABILITY: 2508

81811-01 INSPECTION OBJECTIVES

To determine if the NRC authorized entities information protection system 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 prevents unauthorized disclosure. This is inclusive of control of SGI information provided to applicants and vendors by the NRC, for example, when the NRC forcing function is provided for use in a design specific aircraft impact assessment.

81811-02 INSPECTION REQUIREMENTS

General Guidance.

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 consider conducting a review of past SGI program inspection reports for the facility. During this review the inspector should consider previously inspected requirements in the selection process in an effort to ensure requirements have been inspected.

Inspector(s) are responsible for ensuring the inspection procedure is completed and evaluated to a level which provides assurance that Design Certification (DC) applicants/vendors are meeting the U.S. Nuclear Regulatory Commission (NRC) requirements within 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 NRC authorized entities 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. Completion of other recommended actions contained in this guidance should not be viewed as mandatory; prior to the inspector determining whether an inspection sample has been adequately addressed. Should questions arise regarding procedural requirements or guidance, the inspector(s) should consult with the Office of New Reactor (NRO), Division of Construction, Inspection, and Operational Programs (DCIP) or the Office of Nuclear Security and Incident Response (NSIR), for clarification.

The inspector(s) should coordinate the conduct of the inspection with the NRC authorized entities 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 NRC authorized entities 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 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).

One hour has been allocated within the resource estimate of this inspection procedure for the inspector(s) to conduct SGI program status verifications. The purpose of the status verification is to ensure that the implementation of the DC applicant/vendor program is maintained in accordance with regulations, DC applicant/vendor security plans and implementing procedures.

02.01 Information Protection System.

Verify that the DC applicant/vendor 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 73.21(b)(2))

Specific Guidance.

For the inspection of this requirement, the inspector(s) should verify that the DC applicant/vendor 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 NRC authorized entities 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 NRC authorized entities implementing procedures for the control, protection, and designation of SGI to verify that the DC applicant/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(s) may request that the DC applicant/vendor provide a listing of personnel who have been authorized access to SGI and query DC applicant/vendor security management pertaining to the job description of these personnel which requires that they maintain access to SGI.

02.03 Protection of SGI.

a. Verify that the DC applicant/vendor 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 DC applicant/vendor 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 DC applicant/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. Verify that access to the combination 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))

Specific Guidance.

For the inspection of this requirement, the inspector(s) should query DC applicant/vendor 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 DC applicant/vendor 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 NRC authorized entities implementing procedures for the control, protection and designation of SGI to ensure the DC applicant/vendor 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 DC applicant/vendor 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 NRC authorized entities 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 DC applicant/vendor uses for the development and processing of SGI. The inspector(s) should request that the DC applicant/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. Verify that the NRC authorized entities 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 DC applicant/vendor 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 DC applicant/vendor 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 DC applicant/vendor procedures for the reproduction or transmission of SGI utilizing technology such as copy machines or FAX machines to ensure that the DC applicant/vendor 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 DC applicant/vendor procedures and do not allow unauthorized access and reproduction.

e. Verify that the NRC authorized entities 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 DC applicant/vendor 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 & .22)

Specific Guidance.

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. Verify that the NRC authorized entities 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 DC applicant/vendor 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))

b. Verify that the NRC authorized entities 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))

Specific Guidance.

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 containing SGI however must be properly marked to indicate the designation of the information contained therein.

02.07 Processing, Reproducing, and Transmitting SGI.

Except under emergency or extraordinary conditions, verify that the NRC authorized entities 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 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.

2.08 Removal from SGI Category and SGI Destruction.

a. Verify that the DC applicant/vendor 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 NRC authorized entities 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 NRC authorized entities 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 DC applicant/vendor 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 DC applicant/vendor procedures to verify that the DC applicant/vendor has established measures for the destruction of SGI when the information is no longer needed and that 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.

02.09 Reviews.

Events and Logs. Review DC applicant/vendor 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.

Safeguard Information Program Reviews. Verify that the DC applicant/vendor is conducting reviews of their SGI program.

Problem Identification and Resolution of Problems. Verify that the DC applicant/vendor identifies problems with the protection of SGI program and enters the problems in the corrective action program, as appropriate for SGI topics. Verify that the DC/Vendor has appropriately resolved the regulatory requirement issue for a selected sample of problems with protection of SGI.

Specific Guidance.

The inspector(s) should review safeguards log entries, DC applicant/vendor condition reports, DC applicant/vendor corrective action program entries, etc., for the previous 12 months to determine whether the DC applicant/vendor has experienced issues with the implementation of its SGI program. The inspector(s) should follow-up on issues identified to ensure the DC applicant/vendor 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 DC applicant/vendor to ensure the continued effectiveness of its SGI program.

02.10 Marking of SGI.

a. Verify that the DC applicant/vendor 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))

Specific Guidance.

No inspection guidance.

b. Verify that the NRC authorized entities 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.

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 containing SGI however must be properly marked to indicate the designation of the information contained therein.

81811-03 PROCEDURE COMPLETION

Inspector(s) should attempt to ensure that a requirement from each inspectable area identified in the inspection procedure is completed triennially.

81811-04 RESOURCE ESTIMATE

The resource estimate is approximately 6 hours of direct inspection effort.

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 and Feedback Resolution Accession Number (Pre-Decisional, Non-Public)
N/A	ML16126A125 09/06/16 CN 16-022	Initial issuance. Completed 4 year search for commitments and found none.	None	ML16126A121