INSPECTION PROCEDURE 81421

FIXED SITE PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL OF MODERATE STRATEGIC SIGNIFICANCE

Effective Date: February 7, 2024

PROGRAM APPLICABILITY: IMCs 2600 and 2681

81421-01 INSPECTION OBJECTIVES

01.01 To verify and assess the licensee's implementation of its physical protection system that will minimize the potential for unauthorized removal of Special Nuclear Material (SNM) and facilitate the location and recovery of missing SNM.

01.02 To verify the licensee's implementation of its physical protection program in accordance with U.S. Nuclear Regulatory Commission (NRC) requirements, NRC approved security plans, and any additional NRC site-specific security measures.

81421-02 INSPECTION REQUIREMENTS

General Guidance

In preparing to complete this procedure, the inspector(s) will need to familiarize themselves with relevant documentation which may include, but is not limited to, the licensee's security plan, safety evaluation report (SER), and any site-specific procedures. Specifically, the inspector(s) should apply additional attention to the NRC approved SER and security plan. The SER and security plan may contain additional site-specific security measures that were added as license conditions to the licensee. Site-specific security measures that are added into the licensee's license are based on the type and quantity of SNM that is possessed by the licensee. Section 03.07 provides examples of site-specific security measures that might be added as a condition to the licensee's license. The inspector(s) will need to review the licensee's SER and security plan to identify if any site-specific security measures were assigned to the licensee.

The inspector(s) will conduct tests of security equipment as necessary to validate the effectiveness of the security system and to ensure compliance with the requirements. The inspector(s) may request that a test be conducted as long as it will not reduce facility safety or security, result in a violation of requirements or industry standards, or jeopardize the safety of the inspector(s) or licensee employees. Prior to conducting a test, the inspector(s) must request the test through licensee management and arrange to have a licensee employee conduct the test while the inspector(s) observes. Listed under some of the inspection requirements, the inspector(s) will find guidance on how to inspect the requirement. The guidance does not represent regulatory requirements but is intended to assist the inspector(s) in measuring the licensee's performance.

03.01 Use and Storage

a. Verify that nonexempt[1] SNM is used only within a Controlled Access Area (CAA) and is stored only within an additional CAA such as a vault-type room or approved security cabinet or the equivalent (10 CFR 73.67(d)(1) and (2)).

Specific Guidance

To inspect this requirement, the inspector(s) should walkdown the CAA where the licensee uses SNM. The CAA may be of temporary or permanent construction. Additionally, the inspector(s) should walkdown where the licensee stores SNM. The inspector(s) should verify that the vault type room or container is designed in a way that will delay the theft of the material or facilitate the location and recovery of the material if it is stolen. A CAA has two elements. First, a barrier to isolate the SNM from individuals that are not authorized access to the SNM; and second, an access authorization system such that only individuals that have authorized access can enter the CAA.

Verify the physical structure, equipment, and procedures are adequate to allow the licensee to control access to the CAA.

b. Verify the licensee's physical protection program assures the proper placement and transfer of custody of SNM (10 CFR 73.67(a)(2)(iii)).

Specific Guidance

The inspector(s) should review the licensee's procedures to ensure that they are sufficiently detailed on the placement and transfer of custody of SNM. The procedures should inform the users of their responsibilities and should be revised, as necessary. These activities are also linked to the material control and accounting program.

03.02 Detection and Surveillance

a. Verify the licensee's physical protection program is capable of meeting the general performance objectives of 10 CFR 73.67(a)(1)(i) and (ii) by:

[1] In accordance with 10 CFR 73.67(b)(1), a licensee is exempt from the requirements of this section to the extent that the licensee possesses, uses, or transports (i) SNM which is not readily separable from other radioactive material and which has a total external radiation level in excess of 1 gray per hour at a distance of 1 meter from any accessible surface without intervening shielding, (ii) sealed plutonium-beryllium neutron sources totaling 500 grams or less contained plutonium at any on site or contiguous sites, (iii) plutonium with an isotopic concentration exceeding 80 percent in plutonium-238. Additionally, in accordance with 10 CFR 73.67(b)(2), a licensee who has quantities of SNM equivalent to SNM of moderate strategic significance distributed over several buildings may, for each building which contains a quantity of SNM less than or equal to a level of SNM of low strategic significance, protect the material in that building under the lower classification physical security requirements. Additional reference: 10 CFR 73.67(d), "Fixed site requirements for special nuclear material of moderate strategic significance."

1. Providing early detection and assessment of unauthorized access or activities within the CAA (10 CFR 73.67(a)(2)(i)).

2. Providing early detection of removal of SNM from the CAA (10 CFR 73.67(a)(2)(ii)).

Specific Guidance

Determination of early detection of unauthorized access, activities, or removal of SNM from CAAs will be based on an assessment of the magnitude of the consequences associated with possible misuse of the type and quantity of material that could be removed in a theft attempt. For SNM of moderate strategic significance, two distinct cases are considered:

1. Theft of strategic special nuclear material (SSNM)

2. Theft of Low Enriched Uranium (LEU)

Thefts from a single facility of SSNM in quantities of moderate strategic significance are limited, by definition, to quantities that could not be used to construct a nuclear explosive device; thefts of similar quantities of material from several different facilities could, however, lead to the accumulation of an aggregate quantity that would permit such illicit use. The NRC believes that there are detection systems and procedures that would allow the licensee to detect a theft of SSNM within approximately 2 hours.

Gross theft of Low Enriched Uranium (LEU) refers to thefts in sufficiently large quantity that could yield, upon further enrichment or other processing, enough material of the type and quantity needed to construct an improvised explosive/ nuclear device.

Minor theft of LEU refers to thefts involving much smaller quantities of LEU that could be removed by one or two persons in a private vehicle or on one's person. These minor thefts are significant only to the extent that they could be repeated periodically to eventually accumulate an aggregate quantity that might be obtained in a gross theft.

Licensees who possess less then gross quantities of LEU need not provide for early detection of a single theft of a gross quantity, but the capability for detecting multiple thefts is as important as it is for those licensees possessing gross quantities.

b. Verify the licensee's physical protection system provides indications of an unauthorized removal of SNM and then notifies the appropriate response force of its removal to facilitate its recovery (10 CFR 73.67(a)(2)(iv)).

Specific Guidance

No inspection guidance.

c. Verify that CAAs are sufficiently illuminated and monitored with intrusion alarms or other devices or procedures to detect and observe unauthorized penetrations and/or activities (10 CFR 73.67(d)(1), (2), and (3)).

Specific Guidance

If the licensee uses alarms or other devices to monitor the CAAs when they are unoccupied, the inspector(s) should verify that the alarms or devices are of the

appropriate type, number, and installed in a manner to ensure detection of unauthorized penetrations and/or activities consistent with the alarms or other devices operating manual.

To inspect this requirement, the inspector(s) should visually inspect the licensee's CAAs. Illumination should be sufficient enough to allow detection and surveillance of unauthorized penetration or activities within the CAA where the material is used. The use of high-intensity lighting is not required throughout the CAA. The inspector(s) should verify that lighting is sufficiently uniform throughout the CAA to ensure that material or unauthorized personnel cannot be secreted in a darkened area until a time more convenient for the unauthorized removal of the material. For a facility where experiments must be conducted in a darkened room, the lighting requirement is exempted for as long as is needed provided access control is ensured and the material is accounted for at the end of the experiment.

If the licensee has procedures in place to detect and observe unauthorized penetrations and/or activities in the CAAs the inspector(s) should verify that the procedures are written and implemented in a manner that provides an equal level of protection.

While inspecting this requirement, the inspector(s) should verify that the alarms, devices, and security patrols used to monitor the CAA are adequate to allow the security organization to respond to the threats of theft or thefts of these materials. Additionally, the inspector(s) should verify that all individuals whose duties include the use of procedures are adequately trained in their execution.

03.03 Access Control

a. Verify the licensee's CAAs are clearly demarcated, access is controlled and affords isolation of the material or persons within it (10 CFR 73.2).

Specific Guidance

No inspection guidance.

b. Verify the licensee conducts screening on individuals prior to granting unescorted access to the CAA where material is used or stored, in order to obtain information on which to base a decision to permit such access (10 CFR 73.67(d)(4)).

Specific Guidance

To inspect this requirement, the inspector should verify that the licensee has written criteria for conducting screening including what is acceptable and not acceptable for approving access to the CAA. The inspector(s) should review the licensee's procedures, records, and practices to verify the licensee conducts screening on individuals who are granted unescorted access to CAAs. The inspector(s) should select a sample of individuals who are granted unescorted access to CAAs and verify that the licensee conducted screening prior to granting unescorted access.

The licensee's screening program should be able to uncover information about the individual that would be considered inimical to the safe and secure operation of the facility. An acceptable screening program should consist of past employment, education records, and reference checks.

c. Verify the licensee maintains a controlled badging and lock system to identify and limit access to the CAA to authorized individuals (10 CFR 73.67(d)(5)).

Specific Guidance

To inspect this requirement, the inspector(s) should review the licensee's badging process, and lock and key system. The purpose of the badging system is to facilitate the identification of authorized individuals and the control of access to or within the CAA. The inspector(s) should ensure that information on the badge should be such that it is possible to clearly distinguish personnel authorized for access to the CAAs from those that require an escort. Additionally, the inspector(s) should ensure the locks that are used to control access to CAAs are resistant to manipulation or picking and should not be mastered. Examples of typical lock systems that fit this description are three-position dial-type combination locks, six-pin key locks, and card-key lock systems.

The inspector(s) should review the licensee's process and procedures for assigning keys and combinations to individuals and verify that only authorized personnel have access to such items. The inspector(s) should verify that locks and combinations are changed when information is obtained that the lock system may have been compromised.

d. Verify the licensee limits access to the CAAs to authorized or escorted individuals to require access to perform their duties (10 CFR 73.67(d)(6)).

Specific Guidance

To inspect this requirement, the inspector(s) should observe how the licensee physically controls personnel access into the CAA. The following are some examples of how the licensee can physically control access:

1. control by an authorized person

2. keycard, cipher, combination, or key-lock control system

3. control by security organization

e. Verify that all visitors in the CAAs are under the constant escort of an individual who has been authorized access to the area (10 CFR 73.67(d)(7)).

Specific Guidance

To inspect this requirement, the inspector(s) should review the licensee's procedures and processes for visitors who are escorted into the CAA. The purpose of the escort is to prevent unauthorized activities by the visitor. The type of CAA, the form and amount of the material within it, the activities conducted in the CAA, and the number of authorized individuals within it at any given time will determine how close the escort must be to the visitor.

The inspector(s) should verify the licensee's visitor to escort ratios are for CAAs are implemented as described in its security plans and implementing procedures.

03.04 Response

a. Verify the licensee has a security organization consisting of at least one watchperson per shift who is able to assess and respond to any unauthorized penetrations or activities in the CAAs (10 CFR 73.67(d)(8)).

Specific Guidance

To inspect this requirement, the inspector(s) should review the licensee's security organization and interview members of the security organization to include watchperson(s) as to how they would respond to any unauthorized activities in the CAA. During the conduct of these interviews, the inspector(s) should verify that members of the security organization understand their assigned duties and verify personnel are fully trained and qualified to perform those duties.

Additionally, the inspector(s) should verify the effectiveness of the security organization. The licensee should have processes and procedures documented to ensure that members of the security organization are knowledgeable of their duties (e.g., someone is available to assess alarms or unauthorized penetrations or activities, and if warranted, capable of making notifications to the NRC, local law enforcement agency (LLEA), and the responsible person in licensee management).

An acceptable response force could be LLEA.

b. Verify the licensee has communication capability between the security organization and the appropriate response force (10 CFR 73.67(d)(9)).

Specific Guidance

No inspection guidance.

c. Verify the licensee has response procedures for dealing with threats of theft or theft of SNM (10 CFR 73.67(d)(11)).

Specific Guidance

To inspect this requirement, the inspector(s) should review the licensee response procedures. The procedures must be capable of explaining to a reasonably well-trained individual what steps must be taken to achieve the desired result. Therefore, if the intent of a particular procedure is to notify the LLEA, it must contain telephone numbers or the instruction for use of equipment other than the telephone. The inspector(s) should have an individual who would be responsible for implementing the response procedure demonstrate how they would implement the procedure during the course of their duties.

03.05 Search

a. Verify the licensee conducts searches for SNM on a random basis for vehicles and packages leaving the CAAs (10 CFR 73.67(d)(10)).

Specific Guidance

To inspect this requirement, the inspector(s) should observe (if possible) searches of vehicles and packages leaving the CAA. The inspector(s) should pay particular attention

to how the searches are being conducted. The licensee should be conducting searches in a manner that that would detect the appropriate size, shape, and radiation level of material that is found in the facility. The purpose of the search is to detect gross thefts and minor thefts of material.

03.06 Records

a. Verify the licensee retains a copy of the effective security plan as a record for 3 years after the close period for which the licensee possesses the SNM under each license for which the original plan was submitted (10 CFR 73.67(c)(1)).

Specific Guidance

To inspect this requirement, the inspector(s) should look at how the licensee retains regulatory required records.

b. Verify the licensee retains copies of superseded security plans for 3 years after each change (10 CFR 73.67(c)(1)).

Specific Guidance

No inspection guidance.

c. Verify the licensee retains a copy of response procedures dealing with threats of theft or thefts of SNM. Additionally, verify the licensee retains copies of all superseded response procedures for a period of 3 years after each change. (10 CFR 73.67(d)(11)).

Specific Guidance

To inspect this requirement, the inspector(s) should look at how the licensee retains regulatory required records.

03.07 Examples of Additional Site-Specific Security Measures

a. Physical Barriers

Specific Guidance

The inspector(s) should verify that any openings in any barrier are secured and monitored to prevent exploitation of the opening.

b. Access Controls

Specific Guidance

The licensee must ensure that the individuals granted unescorted access to SNM are trustworthy and reliable. Before granting access into a CAA, licensees must confirm the identity of individuals and verify the authorization for access of individuals, vehicles, and materials. The access authorization program must be consistent with the following requirements:

- 10 CFR 73.57, “Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to Safeguards Information,”

- 10 CFR 73.59, “Relief from fingerprinting, identification and criminal history records checks and other elements of background checks for designated categories of individuals;” and

- 10 CFR 73.61, “Relief from fingerprinting and criminal history records check for designated categories of individuals permitted unescorted access to certain radioactive material or other property.”

Licensees must complete an initial trustworthiness and reliability assessment of individuals seeking unescorted access authorization. The scope of the assessment must encompass at least the 7 years preceding the date of the background investigation or since the individual’s 18th birthday, whichever is shorter. The assessment must include at a minimum:

- Consideration of criminal history based on fingerprinting and a Federal Bureau of Investigation identification and criminal history records check in accordance with 10 CFR 73.57.

- Verification of the true identity of the individual who is applying for unescorted access to ensure that the applicant is who he or she claims to be.

- Verification of employment history, including military history.

- Verification of the individual’s educational history; and

- Consideration of an individual’s character and reputation determination. Licensees must complete reference checks to determine the character and reputation of the individual who has applied for unescorted access.

Based on this assessment, licensees must determine that the individuals granted unescorted access to SNM are trustworthy and reliable. The licensee must document the basis for concluding whether or not an individual is trustworthy and reliable.

Access control portals must be equipped with locking devices and surveillance equipment. Licensees must exercise control over all vehicles inside the CAA to ensure that they are used only be authorized individuals and for authorized purposes.

Licensees must ensure that all escorts of individuals not granted unescorted access but that still require access to CAAs have a means of timely communication with security personnel to summon assistance if needed.

c. Search

Specific Guidance

Licensees must randomly search personnel, vehicles, and materials before they enter and exit CAAs. The frequency and methods of searches must consider the forms of the SNM.

d. Detection and Assessment

Specific Guidance

The physical protection program must include surveillance, observation, and monitoring as needed to satisfy the general performance objectives of 10 CFR 73.67(a). The physical protection program must also include methods to identify indications of tampering. Upon detection of tampering, licensees must initiate response in accordance with security plans and security implementing procedures.

Security patrols must periodically check external areas of the CAAs to include physical barriers.

The licensee must provide a continuously staffed alarm station to perform the following functions: detect and assess alarms; initiate and coordinate adequate response to an alarm; summon off-site assistance; and support command and control. The alarm station must be located in a CAA and must not be visible from the perimeter of the CAA.

The CAA barrier must be monitored by intrusion detection equipment designed to provide uninterrupted visual and audible alarms for the CAA barrier and support the initiation of a timely response.

Intrusion detection equipment transmission lines must be tamper-indicating and self-checking.

Intrusion detection and assessment equipment at vault-type rooms must remain operable from an uninterruptible power supply in the event of the loss of normal power.

e. Communication

Specific Guidance

The alarm station must be capable of two-way voice communication either directly or through an intermediary to local law enforcement using two independent means that use different technologies.

All on-duty security force personnel must be capable of maintaining continuous communication with an individual in the alarm station.

Non-portable communications equipment must remain operable from independent power sources in the event of loss of normal power.

f. Response

Specific Guidance

To the extent practicable, licensees should document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities. To the extent practicable, licenses must conduct annual local law enforcement site familiarization activities to include a review of the protective strategy, onsite and offsite response procedures, and joint response exercises.

Licensees should establish, maintain, and implement a threat warning system that identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat. Licensees must ensure that the specific protective measures and actions identified for each threat level are consistent with the security plan and other emergency plans and procedures. Upon notification by an authorized NRC representative, licensees must implement the specific protective measures based on the threat.

Upon receipt of an alarm or other indication of a threat, licensees should determine the existence and level of the threat in accordance with pre-established assessment methodologies, initiate response actions to promptly detect attempts to remove SNM and notify local law enforcement agencies to recover the SNM in accordance with security implementing procedures.

g. Maintenance and Testing

Specific Guidance

Licensees must establish, maintain, and implement a maintenance, testing, and calibration program to ensure that security systems and equipment including secondary and uninterruptible power supplies are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

03.08 Notifications

a. Verify the licensee notifies the NRC Operations Center as soon as possible but no later than 1 hour after time of discovery of a significant facility security event (10 CFR 73.1200(c)).

Specific Guidance

No inspection guidance.

b. Verify the licensee notifies the NRC Operations Center within 4 hours after time of discovery following facility security events (10 CFR 73.1200(e)).

Specific Guidance

No inspection guidance.

c. Verify the licensee notifies the NRC Operations Center within 8 hours after time of discovery following facility security program failures (10 CFR 73.1200(g)).

Specific Guidance

No inspection guidance.

d. Verify that within 60 days of making a report in accordance with 73.1200, the licensee submits a written report to the NRC (10 CFR 73.1205).

Specific Guidance

To inspect this requirement, the inspector(s) should review any written reports submitted by the licensee and ensure the report contains sufficient information for NRC analysis and evaluation.

03.09 Events

a. Verify the licensee maintains a current log and records the safeguards events within 24 hours of discovery (10 CFR 73.1210).

Specific Guidance

To inspect this requirement, the inspector(s) should review and evaluate licensee event reports and safeguards log entries since the last inspection.

81421-04 RESOURCE ESTIMATE

The resource estimate for the completion of this procedure consists of approximately 24 hours for the inspection.

81421-05 PROCEDURE COMPLETION

The frequency of at which this inspection activity is to be conducted is triennially (once every 3 years).

81421-06 REFERENCES

NUREG/CR-0027, “Capability for Intrusion Detection at Nuclear Fuel”

NUREG-0320, “Interior Intrusion Alarm Systems”

NUREG/CR-0360, “Physical Protection of Nuclear Facilities”

NUREG/CR-2492, “Special Nuclear Material Self-Protection Criteria Investigation”

RG 5.7, “Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas”

RG 5.12, “General Use of Locks in the Protection and Control of Facilities and Special Nuclear Material”

RG 5.59, “Standard Format and Content for a Licensee Physical Security Plan for the Protection of Special Nuclear Material of Moderate or Low Strategic Significance”

END

Attachment 1: Revision History for IP 81421

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	11/23/09 CN 09-028	This document has been revised to: (1) emphasize the risk-informed, performance-based approach to inspection, (2) impose changes to inspection activities due to orders issued that have not been incorporated by rulemaking. Completed 4-year historical CN search.	N/A	N/A
	ML23172A268 02/07/24 CN 24-006	This document has been revised to ensure it is applicable to Category II fuel cycle facilities and up to date with current regulations and orders. Upon completion of a SUNSI review, the staff concluded that this document should be de-controlled. Consistent with the staff's SUNSI determination, this document has been de-controlled and the SUNSI markings have been removed.	N/A	ML23192A824