INSPECTION PROCEDURE 81601

FIXED SITE PHYSICAL PROTECTION OF FORMULA QUANTITIES OF STRATEGIC SPECIAL NUCLEAR MATERIAL – NON-POWER REACTORS

Effective Date: 06/01/2020

PROGRAM APPLICABILITY: IMC 2545

This inspection procedure (IP) is applicable to all U.S. Nuclear Regulatory Commission (NRC) licensed non-power reactors that possess formula quantities (FQ) of non-exempt strategic special nuclear material (SSNM).

81601-01 INSPECTION OBJECTIVES

The objectives of this IP are 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 Plans and Procedures. To assure that the licensee has a program that will implement regulatory requirements and license conditions related to the protection of FQ of SSNM.

01.02 Access Control. To assure that the licensee has a system that will limit access to the controlled access areas (CAA), material access areas (MAA), vital areas (VA), and protected areas (PA) to authorized individuals.

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 unescorted access.

01.04 Physical Protection System. To assure that the licensee has a physical protection system that will: 1) minimize the potential for unauthorized removal of SSNM; and, 2) facilitate the location and recovery of missing SSNM.

01.05 Response. To assure that the licensee has an organization that will assess and respond to unauthorized penetrations or activities in the CAA, MAA, VA, and PA.

81601-02 INSPECTION REQUIREMENTS

02.01 Plans and Procedures.

a. Plans.

1. Determine whether the licensee is continuing to implement the provisions in the NRC-approved physical security plan (PSP). [10 CFR 50.34(c), 10 CFR 73.67(c)(1)]

2. Determine whether the licensee has established, followed, and maintained an NRC-approved safeguards contingency plan (SCP). [10 CFR 50.34(d), 10 CFR 73 Appendix C]

b. Revisions. Determine whether the licensee made any revisions to the NRC-approved PSP or SCP consistent with provisions in the regulations.

1. Verify that the licensee submitted an application for an amendment to the license for any changes that decrease the effectiveness of the NRC-approved PSP or SCP. [10 CFR 50.54(p)(1)]

2. Verify that the licensee maintained records of any changes that did not decrease the effectiveness of the NRC-approved PSP or SCP for a period of three years from the date of the change. [10 CFR 50.54(p)(2)]

3. Verify that the licensee submitted a report containing a description of any changes that did not decrease the effectiveness of the NRC-approved PSP or SCP within two months from the date of the change. [10 CFR 50.54(p)(2)]

c. Implementing Procedures.

1. Verify whether the licensee is implementing the provisions in the NRC-approved PSP or SCP through any potentially required security procedures. [10 CFR 73.67(c)(2), 10 CFR 73 Appendix C]

2. Verify that the licensee is maintaining written response procedures for dealing with theft or threat of theft of SNM. [10 CFR 73.67(d)(11), 10 CFR 73 Appendix C]

d. Reviews. Determine whether the licensee is conducting periodic reviews or assessments of the security program.

e. Records. Determine whether the licensee is maintaining records consistent with the provisions in the NRC-approved PSP, SCP, or applicable requirements in the regulations. [10 CFR 50.54(p)(2), 10 CFR 73.67(c)(1), 10 CFR 73.70]

02.02 Access Authorization.

a. Background Screening. Verify that the licensee conducts screening of individuals prior to granting unescorted access to the CAA, MAA, VA, or PA. [10 CFR 73.67(d)(4)]

b. Criminal History Records Check. Verify that the licensee meets the requirements regarding fingerprinting individuals who are seeking or permitted: 1) unescorted access to VAs; or 2) unescorted access to SNM.

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

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

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

4. Verify that the licensee obtains fingerprints for a criminal history records check for each individual who is seeking or permitted: 1) unescorted access to VAs; or 2) unescorted access to SNM. [10 CFR 73.57(g)(2)]

c. 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. [10 CFR 73.57(g)(1)]

02.03 Access Control.

a. Use and Storage.

1. Verify that the licensee is storing or processing SSNM only within MAAs. [10 CFR 73.60(a)(1)]

2. Verify that the only activities requiring access to SSNM or equipment employed in the process, use, or storage of SSNM are permitted in MAAs. [10 CFR 73.60(a)(1)]

3. Verify that all MAAs are located within the PA. [10 CFR 73.60(a)(2)]

4. Verify that the licensee is storing SSNM not in process only in a vault equipped with an intrusion system or in a vault-type room controlled as a separate MAA. [10 CFR 73.60(a)(3)]

5. Verify that the licensee is using SNM only within a CAA. [10 CFR 73.67(d)(1)]
6. Verify that the licensee is storing SNM only within a CAA. [10 CFR 73.67(d)(2)]

7. Verify that the licensee's safeguards system assures proper placement and transfer of custody of SNM. [10 CFR 73.67(a)(2)(iii)]

b. Badging and Lock System. Verify that the licensee has a system to identify and limit access to the CAA, MAA, VA, and PA to authorized individuals. [10 CFR 73.67(d)(5)]

c. Limiting Access. Verify that the licensee is limiting access to authorized or escorted individuals. [10 CFR 73.60(a)(5), 10 CFR 73.67(d)(6)]

d. Escorts. Verify that the licensee has authorized individuals escorting all visitors inside the CAA. [10 CFR 73.67(d)(7)]

e. Search.

1. Verify that the licensee has a process to conduct package searches prior to entry into MAA to ensure items such as firearms, explosives, incendiary devices, or counterfeit substitute items which could be used for theft or diversion of SNM. [10 CFR 73.60(a)(6)]

2. Verify that the licensee has a process to conduct exit searches of individuals, packages, or vehicles to detect the presence of concealed SNM. [10 CFR 73.60(b)]

3. Verify that the licensee has a process to conduct random CAA exit searches of vehicles and packages for concealed SNM. [10 CFR 73.67(d)(10)]

f. Postings. Verify that the licensee has the required posting of notices/warnings in required locations. [10 CFR 73.75]

02.04 Physical Protection System.

a. Detection and Surveillance.

1. Verify that all unoccupied MAAs are locked and protected by an active intrusion alarm system. [10 CFR 73.60(c)]

2. Verify that the licensee has methods to observe individuals in MAAs to assure that SNM is not diverted. [10 CFR 73.60(a)(7)]

3. Verify that the licensee can provide early detection and assessment of: 1) unauthorized activities in the CAA; and, 2) removal of SNM from the CAA. [10 CFR 73.67(a)(2)(i), 10 CFR 73.67(a)(2)(ii)]

4. Verify that the licensee can monitor the CAA to detect unauthorized penetration or activities. [10 CFR 73.67(d)(3)]

b. Maintenance and Testing.

1. Verify that the licensee maintains all intrusion alarms, physical barriers, and other devices used for material protection in an operable condition. [10 CFR 73.60(d)(1)]

2. Verify that the licensee inspects and tests each intrusion alarm for operability and required functional performance at the beginning and end of each interval of use, but at least once every seven days of use. [10 CFR 73.60(d)(2)]

3. Verify that the licensee periodically tests all security-related devices and equipment for operability.

02.05 Response.

a. Organization. Verify that the licensee has at least one watchman per shift that will assess and respond to any unauthorized penetrations or activities in the CAA. [10 CFR 73.67(a)(2)(iv), 10 CFR 73.67(d)(8)]

b. Communication. Verify that the licensee has communication capability between the security organization and the appropriate response force. [10 CFR 73.67(a)(2)(iv), 10 CFR 73.67(d)(9)]

c. Procedures. Verify that the licensee has response procedures for dealing with threats of theft and theft of SNM. [10 CFR 73.67(d)(11)]

81601-03 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 inspector should note that implementation of these requirements at non-power reactors vary widely and requires site-specific consideration when evaluating these elements.

Additionally, the inspector should be aware that any written inspection notes, related to the specific details of how a licensee is in compliance with the regulatory requirements, could be considered Law Enforcement Sensitive, Safeguards Information, or Safeguards Information – Modified Handling. Care should be exercised to avoid recording site-specific details and instead use general statements related to compliance with the regulations, NRC-approved PSP, or other commitments.

It is not anticipated that a licensee will possess a FQ of non-exempt SSNM. Over the years, the NRC took steps to reduce the amount of non-exempt SSNM, in the form of unirradiated reactor fuel, that a licensee could possess through license conditions and Orders. Most of the licensees that possess quantities of exempt SSNM, in the form of irradiated reactor fuel, ship the material before it will become non-exempt.

03.01 Plans and Procedures.

Licensees typically have a license condition requiring adherence to an NRC-approved PSP and SCP. Some licensees may incorporate the requirements for an SCP into the PSP. While the regulations do not require periodic updates of the NRC-approved PSP and SCP, the licensee is still required to be in compliance with all regulations that may have been affected by rulemaking since the last update to the NRC-approved PSP and SCP. In the absence of a requirement or license condition, the inspector should also be aware that compliance may also be demonstrated through adherence to procedures or processes.

If a change to the NRC-approved PSP and SCP does not decrease the effectiveness of the plan, the licensee does not have to submit the change to the NRC for prior approval using the license amendment process. However, the licensee is required to have determined before implementation that the change does not decrease plan effectiveness. If the change does not decrease plan effectiveness, the change needs to be submitted within two months after implementation. Changes that are determined by the NRC to reduce overall effectiveness of

the plan can result in the licensee being cited not only for a failure to comply with the appropriate requirements, but also for failure to apply for and receive approval of such change prior to implementation.

Licensees may have developed procedures in addition to the response procedures discussed below. Some licensees may have a requirement in the license, technical specifications, PSP, or SCP to develop security plan implementing procedures. If applicable, the inspector should review a sample of procedures, forms, checklists, etc. that may be used to implement the provisions contained in the regulations or the NRC-approved PSP and SCP.

Although regulations do not require the licensee to perform a review of the physical security program, such a review would be desirable to assess the current efficiency and assure the continued efficiency of the program. The inspector should be aware that licensees may have a TS, PSP, or SCP requirement to conduct a review.

Licensees are required to maintain records of changes to the NRC-approved PSP and SCP made under 10 CFR 50.54(p) for a period of three years from the date of the change. The licensee is also required to maintain a copy of the effective PSP and SCP as a record for three years after the SNM is removed from the site.

Additionally, the licensee is required to maintain records of the following information: 1) individuals designated as authorized individuals; 2) individuals authorized to have access to SNM, MAAs, VAs, and vital equipment; 3) registers of visitors, vendors, and other individuals not employed by the licensee; 4) log of individuals granted access to vital areas other than the control room; 5) documentation of all routine security tours, inspections, tests, and maintenance; 6) records of each onsite alarm, false alarm, alarm check, and tamper indication, including details of response by guards or watchmen; 7) shipments of SNM; and, 8) procedures for controlling access to PAs and access to keys for locks used to protect SNM.

03.02 Access Authorization.

Licensees are required to conduct screening of individuals prior to granting unescorted access to the CAA, MAA, VA, and PA. The licensee's program for screening should be able to uncover information about the individual that would be considered inimical to the safe and secure operation of the facility. Regulations in 10 CFR 73.67 do not specify the type(s) of screening to perform. Post-9/11, licensees agreed[1] to incorporate enhanced background screening of staff. The inspector should verify that the background screening elements are in accordance with PSP requirements or other commitment.

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: 1) unescorted access to VAs (if applicable); or 2) unescorted access to SNM. In the context of 10 CFR 73.57, unescorted access means solitary access by an individual to a non-power reactor vital area (if applicable) or to SNM in the non-power reactor such that the individual can use or remove the SNM in an unauthorized manner. Prior to being granted unescorted access, an individual must be determined to be trustworthy and reliable based on the results of an 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

[1] Between 2002-2004, NRC issued Confirmatory Action Letters to formalize commitments to incorporate site-specific compensatory measures, which enhanced protection against radiological sabotage or theft.

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.

Licensees are required to have at least one current documented NRC-approved reviewing official who has unescorted access and 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 unescorted access to 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 based on all of the background screening information.

03.03 Access Control.

During a tour of the facility, the inspector should verify that SSNM is: 1) used within a CAA, which may be of temporary or permanent construction; and, 2) stored within an MAA, consisting of a vault-type room or storage container. The CAA, MAA, VA, and PA should be as described in the NRC-approved PSP and 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. Equipment required to handle SSNM and knowledge related to use of the equipment should be protected.

Smaller facilities may have the flexibility to use an existing identification system to control access. Larger facilities with multiple organizations (i.e., reactor operations, health physics, researchers) may have a more sophisticated access control system. Post-9/11, licensees agreed to incorporate improved access controls to key areas within the facilities. The inspector should verify that the access controls are in accordance with PSP requirements or other commitment.

Facilities must control the issuance, restrict the duplication, and control the return of physical access control devices. Periodic inventory should be conducted to verify accounting for issued and stored devices. In the event the licensee has their own locksmith, the inspector may choose to interview the locksmith on processes and conduct a portion of the records review during a visit with locksmith. Records review should indicate that physical access control devices are: 1) granted only to authorized individuals when all regulatory requirements and local processes are completed; and, 2) returned when the device is no longer needed.

Licensees are required to have a controlled system to identify and limit access to the CAA and MAA to authorized individuals. Facilities may utilize a system, process, or procedure to limit access to various categories of authorized or escorted individuals that require access to the CAA and MAA for the conduct of official duties or approved activities. Direct visual surveillance is almost always necessary to allow observation of the visitor's actions. The inspector should verify the means the licensee uses to limit access to the CAA and MAA through observation or reviews.

The inspector should verify that the licensee has a process for conducting searches and that searches are appropriate for the size, shape, and radiation level of material found in the facility. Post-9/11, licensees agreed to incorporate additional vehicle and package searches. The inspector should verify that searches are in accordance with PSP requirements or other commitment.

Licensees are required to post notices at entrances informing individuals that it is a Federal crime to introduce any dangerous weapon, explosive, or other dangerous instrument or material into a facility regulated by the Commission. The posted notices: 1) must be conspicuously displayed at every vehicle and pedestrian entrance; 2) must be easily readable day and night by both pedestrian and vehicle traffic; and, 3) must contain the following required language:

> The willful unauthorized introduction of any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property into or upon these premises is a Federal crime. (42 U.S.C. 2278a.)

The postings may be combined with other information, but are required to contain the above statement. Each licensee has a unique facility layout and compliance with this requirement will vary from facility to facility. Licensees located in a separate structure may consider placing these on the outermost fence line where both vehicles and pedestrians enter. Licensees located inside of a building on a University campus may consider placing these on all doors that afford access into the CAA or other pre-defined security area/zone.

03.04 Physical Protection System.

In order to facilitate a prompt response for the location and recovery of SNM, alarms and other devices are used to monitor the areas when they are unoccupied and therefore must be appropriate in type, number, and application to ensure detection and assessment of unauthorized presence or activities during times when the areas are unoccupied. If procedures are used in place of equipment, the procedures must be written and implemented in a manner that provides an equivalent level of protection. The inspector should verify the devices referenced in the NRC-approved PSP are operable and operating, as required.

The CAAs must be illuminated such that all reasonable paths from openings in the barrier to the SNM can be observed by individuals at work in the CAAs. The illumination levels for normally occupied CAAs should be sufficient to allow surveillance by the unaided human eye. The lighting should be uniform, shadowless, and free from glare.

Licensees must have a PSP or procedural requirement to perform maintenance and testing on equipment and alarms at some frequency (e.g. based on a time frequency or manufacturer's specification) to ensure operability. The inspector should be able to verify that intrusion alarms or other devices or procedures that monitor the areas to detect unauthorized penetration or activities are in working order, provide communication for security response, and are tested periodically for functionality.

The inspector is not expected to test security equipment. However, sometimes a test is necessary to evaluate the effectiveness of the security system and to ensure compliance with requirements. In this situation, the inspector 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 or licensee employees. To conduct the test,

the inspector must request the test through licensee management, and arrange to have a licensee employee conduct the test while the inspector observes. The inspector may decide to observe the alarm test from the point of initiation at the facility or at the point of receipt at the alarm monitoring station. For facilities that do not operate 24 hours a day, the inspector may consider observing deactivation and activation of alarms at the start and conclusion of daily operations.

03.05 Response.

While there are no specific regulatory requirements to form a basis for determining the adequacy of response forces, they should be capable of responding in a reasonable period of time and assisting in the location and recovery of missing or stolen SNM. Licensees typically do not have a self-contained security or response organization, and therefore, rely on local law enforcement (LLEA) or campus-based police officers. The licensee should have an arrangement with these organizations to assess and respond to unauthorized penetrations or activities in the CAA. The inspector may consider touring the local dispatch center or police station. The inspector should be aware that these organizations are typically external to the licensees organizational structure; therefore, resolution of any issues related to regulatory compliance would be the responsibility of the licensee. Post-9/11, licensees agreed to incorporate enhanced coordination with the appropriate local, state, and federal response organizations. The inspector should consider inquiring as to the ongoing coordination of activities between the licensee and response organizations.

Licensees must have and maintain communication capabilities with response organizations. Post-9/11, licensees agreed to incorporate improved external communication systems. The inspector should verify that the communication capabilities are consistent with PSP requirement or other commitment.

Licensees are required to have response procedures dealing with threat of theft of SNM and theft of SNM. The inspector should expect that these procedures or similar procedures are used by the responding organization. The procedures must be capable of explaining to a reasonably well-trained individual what steps must be taken to achieve the desired result.

81601-04 RESOURCE ESTIMATE

For planning purposes, the estimated, direct, onsite inspection effort to complete this inspection procedure is 32 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.

81601-05 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 annually.

81601-06 REFERENCES

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

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

Regulatory Guide 5.52, “Standard Format and Content of a Licensee Physical Protection Plan for Strategic Special Nuclear Material at Fixed Sites (Other than Nuclear Power Plants)”

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

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

END

Attachment:
1. Revision History Sheet for IP 81601

Attachment 1 - Revision History for IP 81601

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)
	ML19190A267 03/13/20 CN 20-015	Initial issue to support inspection of research and test reactor programs described in IMC 2545.	None	ML19205A354