INSPECTION PROCEDURE 81311

PHYSICAL SECURITY REQUIREMENTS FOR INDEPENDENT SPENT FUEL STORAGE INSTALLATIONS

Effective Date: 08/01/2022

PROGRAM APPLICABILITY: IMCs 2201C, 2202B, 2690

81311-01 INSPECTION OBJECTIVES

01.01 Verify the licensee's physical protection program for an independent spent fuel storage installation (ISFSI) is implemented in accordance with the U.S. Nuclear Regulatory Commission (NRC)-approved security plans, regulatory requirements, and any other applicable requirements and orders.

01.02 Determine if the ISFSI physical protection program provides assurance, consistent with regulations in Title 10 of the *Code of Federal Regulations* (10 CFR 73), that activities involving spent nuclear fuel and high-level radioactive waste do not constitute an unreasonable risk to public health and safety.

81311-02 INSPECTION REQUIREMENTS AND GUIDANCE

This inspection procedure (IP) is applicable to ISFSIs licensed under 10 CFR Part 50, Part 52, and Part 72.

This IP is divided into two sections to address the two different types of licenses (general and specific) for the receipt, transfer, packaging, and possession of spent nuclear fuel (SNF) and power reactor-related greater-than-class C (GTCC) waste. (10 CFR 72.2(a)(1))

Spent fuel is stored at an ISFSI located either at an operating power reactor site (i.e., inside the reactor's protected area (PA), in the owner-controlled area (OCA), or in a separate PA), at a decommissioning power reactor site, or at an away-from-reactor (AFR) site using a dry cask storage system (DCSS). In lieu of a DCSS, a wet storage ISFSI may use a spent fuel pool (SFP) as part of a wet storage system to store the spent fuel. This IP will be implemented at an AFR site that is 1) a specifically licensed ISFSI whose associated support programs are not inspected under a 10 CFR Part 50 license, or 2) any generally licensed ISFSI where decommissioning and final survey activities related to reactor operations are completed and the only remaining operation conducted under the 10 CFR Part 50 license is the operation of the general licensed ISFSI.

Section 02.01 through 02.08 applies to a 10 CFR Part 50 or Part 52 licensee issued a general license for an ISFSI under 10 CFR 72.210 of Subpart K. This general license authorizes the use of a DCSS that has been approved in accordance with 10 CFR Part 72 and uses casks listed in 10 CFR 72.214.

Section 02.09 applies to any licensee issued a specific license for an ISFSI under 10 CFR 72.40. Under a specific license, any approved DCSS design can be used at any location. While a specific 10 CFR Part 72 license is independent from a co-located 10 CFR Part 50 reactor license, some structures, systems, and programs that are part of the licensing basis for the reactor license may be shared and subject to different security requirements and or security orders.

In accordance with 10 CFR 73.55(r), “Alternative measures,” for general licenses, the Commission may authorize a licensee to provide a measure for protection against radiological sabotage other than one required by 10 CFR 73.55. Exemptions under 10 CFR 73.5 and 10 CFR 72.7 can be granted by the Commission for both general and specific ISFSI licenses from the requirements in 10 CFR Part 73 and 10 CFR Part 72, respectively. Inspector(s) should review the licensee’s physical security plans that describe any alternative measures authorized and/or any exemptions granted by the Commission. Likewise, in accordance with 10 CFR 73.51(d) for specific licenses, the Commission may, on a specific basis and upon request or on its own initiative, authorize other alternative measures for the protection of spent fuel and high-level radioactive waste subject to the requirements of 10 CFR 73.51 if after evaluation of the specific alternative measures, it finds reasonable assurance of compliance with the performance capabilities of the general performance objectives (10 CFR 73.51(b)). The requirements of 10 CFR 73.21 and 73.22 apply to both general and specific licensees.

This IP establishes a method for inspecting an ISFSI. The primary application is for the inspection of a licensed ISFSI containing cask-stored spent fuel; however, most requirements are also applicable to existing wet storage facilities. Prior to the first loading of SNF, a general license must notify the NRC at least 90 days in advance in accordance with 10 CFR 72.212(b)(1). To promote efficiency, selected portions of this procedure may be conducted as early as practical during construction and installation of security features or components to identify problems early before completion of the work which may make their resolution difficult.

In preparing to complete this procedure, the inspector(s) needs to identify what type of license the licensee has been issued e.g., general license or specific license. Additionally, the inspector(s) should familiarize themselves with relevant documentation which may include, but is not limited to the licensee’s security plans, safety evaluation report (SER), and site-specific and/or corporate procedures. Specifically, the inspector(s) should apply additional attention to the NRC approved SER and any recent security plan changes that could be relevant to the inspection activity. Additionally, the inspector(s) should note that not all inspection requirements are applicable for each ISFSI licensee. The inspector(s) will need to review the licensee’s approved exemptions, alternative measures, physical security plan, and SER to identify any requirements that may not apply. The inspector(s) should note that some requirements may already be inspected under other security inspection programs, (e.g., reactor security baseline inspection program, security decommissioning inspection program) if the inspector(s) identifies elements that are included under another program they do not need to be reinspected under this IP.

This IP applies to ISFSIs located inside an operating reactor PA for its initial inspection. For subsequent inspections, ISFSIs located inside an operating power reactor PA are subject to the security requirements of 10 CFR 73.55 and subject to the baseline security inspection within the reactor oversight program.

General License Requirements and Guidance for Co-Located / AFR ISFSI

02.01 General License Requirements and Guidance.

Under 10 CFR 72.210, a general license is issued for the storage of SNF in an ISFSI at power reactor sites to persons authorized to possess or operate nuclear power reactors under 10 CFR Part 50 or Part 52. Through completion of the inspection activities for this IP, inspector(s) shall verify or determine that the licensee's physical protection program associated with this sample is designed and implemented to protect the SNF against the design basis threat (DBT) of radiological sabotage (10 CFR 72.212(b)(9)) and meet the requirements of site-specific security orders (e.g., interim compensatory measures (ICMs), additional security measures (ASMs)). Inspector(s) should note that ICMs and ASMs are two different documents that encompass the same security requirements. Licensees who had an existing ISFSI prior to September 2007 were issued the ICMs and licensees who built an ISFSI after September 2007 were issued the ASMs.

a. Verify the licensee protects the spent fuel against the DBT of radiological sabotage in accordance with the provisions and requirements as are set forth in the licensee's physical security plan pursuant to 10 CFR 73.55 and the conditions and exemptions under the provisions of 10 CFR 72.212(b)(9) and any site-specific security orders.

Specific Guidance

For this portion of the inspection, the inspector(s) should review the licensee's site security orders, security plan, training and qualification plan, safeguards contingency plan, protective strategy, and relevant implementing procedures and ensure the protection of the ISFSI has been incorporated into the relevant documents. The inspector(s) should consider conducting a review of past security inspection reports for the ISFSI.

b. Verify the licensee's ISFSI physical protection measures do not decrease the effectiveness of the physical protection program for the protection of vital equipment associated with the reactor and SFP required by 10 CFR 73.55. (10 CFR 72.212(b)(9)(i))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's security plans and implementing procedures and conduct interviews with security staff to ensure the ISFSI does not create any decrease in the security effectiveness of the designated vital areas (VAs).

c. Verify the storage of SNF is within a PA, in accordance with 10 CFR 73.55(e), but need not be within a separate VA. Existing PAs may be expanded, or new PAs added for the purpose of storage of spent fuel in accordance with the general license. (10 CFR 72.212(b)(9)(ii))

Specific Guidance

For this requirement the inspector(s) should review the licensee's analysis of their physical barriers (the specific use, type, function, and placement) to verify they meet the physical barrier requirements set forth in 10 CFR 73.55(e), specifically 10 CFR 73.55(e)(8), "Protected Area."

02.02 Search Activities (Personnel, Materials, and Vehicles)

a. Verify the licensee has established measures to observe all vehicle search functions (OCA and PA) in a manner that enables the initiation of a response. (10 CFR 73.55(g)(1)(ii)(C))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's security plans and implementing procedures for the conduct of vehicle search at the OCA and PA vehicle access control points. The OCA vehicle access control points are required to have video surveillance equipment that is monitored by a member of the security organization (other than the armed over-watch officer who is positioned to provide the immediate response) to observe search activities and initiate a response when necessary. The PA vehicle access control point may have either video surveillance equipment used by security force members to monitor the search process and initiate response or may be the subject of direct surveillance by a member of the security organization to monitor the search process and initiate a response if necessary.

b. Verify the licensee subjects all personnel, materials, and vehicles to search prior to granting access to the PA and that the search is conducted in accordance with the regulations, licensee security plans, and implementing procedures. (10 CFR 73.55(h)(3))

Specific Guidance

No inspection guidance.

c. Verify at a minimum, personnel searches are performed by physical pat-down searches or by firearms and explosives detection equipment prior to admission to the PA. (10 CFR 73.55(h)(3)) and (10 CFR 72.212(b)(9)(iii))

Specific Guidance

The inspector(s) should observe the licensee's personnel search process, implemented prior to the licensee granting personnel access to the PA, to verify that the search process is consistent with the licensee's implementing procedures; this guidance only applies to ISFSIs not in the same PA as the reactor. Inspector(s) should verify any approved exemptions for performing visual searches in lieu of physical pat-down searches.

d. Verify the licensee's security measures for excepting materials from the search process includes the clear identification, positive control, storage, and verification of materials in accordance with the regulation, licensee security plans, and implementing procedures. (10 CFR 73.55(h)(3)(v) and 10 CFR 73.55(h)(3)(vi))

Specific Guidance

When inspecting this requirement, the inspector(s) should review the licensee's security plans and implementing procedures for the identification, control, and storage of packages and materials that are exempted from search. The inspector(s) should verify that the licensee implements processes for identification, control, and storage of packages and materials exempted from search in accordance with the regulations,

licensee procedures, and NRC Safeguards Advisory SA-06-04, “Implementing Search Requirements and Approved Exceptions for Packages and Materials at NRC Licensed Facilities.” The vehicles that carry items which may be exempted from search are not exempted from search and must be searched in accordance with the search requirements for the area (OCA, PA) that the vehicle will be entering.

e. Verify the licensee’s security measures for excepting bulk materials from the search process include providing an armed escort for the excepted material when entering the PA area and that the bulk materials are not, to the extent practicable, offloaded adjacent to a VA (if applicable). (10 CFR 73.55(h)(3)(vii) and 10 CFR 73.55(h)(3)(viii))

Specific Guidance

When assessing the licensee’s processes and implementing procedures for the control of packages and materials, the inspector(s) should review the licensee’s security plans and implementing procedures for the control of bulk items. Within this area of the licensee’s procedures, the licensee should address its process for bulk items entering the PA. Bulk items that cannot be searched must be escorted by an armed member of the security organization to the final destination or receiving area where the exempted items are offloaded and verified. The vehicles that carry bulk items are not exempted from search and must be searched in accordance with the search requirements for the area (OCA, PA) that the vehicle will be entering.

f. Verify the licensee implements access denial actions for attempted or suspected introduction of firearms, explosives, and incendiary devices or other items which could be used to commit radiological sabotage in accordance with their security plans and implementing procedures. (10 CFR 73.55(h)(3)(iii))

Specific Guidance

In preparation to inspect the search process, the inspector(s) should familiarize themselves with the licensee’s security plans and implementing procedures for the conduct of personnel, material, and vehicle search. If applicable, the inspector(s) should query the personnel conducting search activities regarding actions and measures taken when search equipment alarms indicating the presence of items the equipment was designed to detect or when search personnel have identified firearms, explosives and incendiary devices, or other items which could be used to commit radiological sabotage during the search process. The inspector(s) should ensure that the actions and measures stated are in accordance with regulations and written procedures. At a minimum the person, material, or vehicle that causes equipment to alarm or is identified through visual search that an item could be a firearm, explosive or incendiary device, or other items which could be used to commit radiological sabotage, the person, material, or vehicle should be denied access and be subjected to further search via visual and physical means to ensure the absence of these items.

g. Verify the licensee has established and implements measures to: (1) ensure that all vehicles in the PA are used for plant functions or emergencies; (2) are operated by personnel with unescorted access to the PA or are escorted in accordance with 10 CFR 73.55(g)(8); (3) have keys removed or are otherwise disabled when not in use. (10 CFR 73.55(g)(3))

Specific Guidance

No inspection guidance.

h. Verify the licensee has established and implements measures to assign armed escorts (armed member of the security organization) to vehicles transporting hazardous materials in the PA. (10 CFR 73.55(g)(3)(iv))

Specific Guidance

No inspection guidance.

02.03 Access Control Points and Access Controls.

a. Verify the licensee has established and implements measures to control keys, locks, combinations, passwords, and related access control devices used to control access to the PA and security systems. (10 CFR 73.55(g)(6)(i))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's security plans and implementing procedures to identify security systems for which the licensee controls access. The security systems that should have access control measures associated with them could be areas such as alarm stations, access badging terminals, or secondary power supplies for alarm annunciation equipment and communications systems which are required by regulation or through the licensee's security plans and implementing procedures. Access controls implemented by the licensee may include equipment or systems that are maintained in a locked area with the specific keys/key cards for entry to the area being controlled. Additionally, the control of passwords that provide access to the functions of a security computer system or an access badging terminal should be controlled.

b. Verify the licensee controls access at each access control point (designed and in use for authorized access) where personnel, materials and vehicles can be brought into the PA in accordance with regulations, licensee security plans and implementing procedures. (10 CFR 73.55(g)(1))

Specific Guidance

When inspecting access control points to ensure the licensee controls all locations where personnel, materials, and vehicles can be brought into the PA, the inspector(s) should familiarize themselves with the licensee's access control measures by reviewing the licensee's security plans and implementing procedures for access controls. The inspector(s) should then identify all access control points in use (i.e., entrance and exit turnstiles, material access portals, vehicle access gates, etc. that are in operation on a daily basis). The inspector(s) should verify that these locations are controlled to ensure that all personnel, materials, and vehicles are identified, authorized, and searched and that additional supporting security measures such as personnel or vehicle escorts (armed or unarmed), security seal verification measures, etc., are implemented in accordance with the regulations, licensee security plans, and implementing procedures. The inspector(s) should also verify that the configuration of these areas (to include the

assigned personnel) does not allow personnel, materials, and vehicles to bypass the search process or measures.

The inspector(s) should be specifically observant of the following: (1) the number of personnel assigned to conduct the access control or search process; (2) the responsibility of personnel assigned to these areas (i.e., overwatch, search function, interim compensatory measure for temporary barrier openings such as vehicle access portals, etc.); (3) the specific location of personnel assigned to these areas especially if designated by procedure; (4) that the configuration and location of equipment and personnel prevent unauthorized bypass of search components and access control equipment or measures; (5) whether personnel assigned to these areas are to be armed with a firearm per regulation and/or procedure; and (6) that the barriers at these locations are secured and are provided intrusion detection when not in use so they cannot be bypassed without being detected.

c. Verify the licensee issues access control devices only to individuals who have unescorted access authorization and require access to perform official duties and responsibilities. (10 CFR 73.55(g)(6)(i)(A))

Specific Guidance.

For the inspection of this requirement, the inspector(s) should request that the licensee print a “current” copy of a PA access list from the security computer system or view an electronic database of the PA access list. The inspector(s) should then request that the licensee make available the records or logs used to document the issuance of access control devices (i.e., keys, locks, etc.). The inspector(s) should compare the access lists to the issue records or log to ensure that the personnel who are provided these devices possess unescorted access and that the personnel’s unescorted access is consistent with the area for which they were issued an access control device.

d. Verify the licensee maintains a record of all personnel to whom access control devices have been issued and implements a process to account for access control devices at least annually. (10 CFR 73.55(g)(6)(i)(B))

Specific Guidance

No inspection guidance.

e. Verify the licensee has established measures to retrieve, change, rotate, deactivate, or otherwise disable access control devices that may have been compromised or when a person with access to access control devices has been terminated under less than favorable conditions. (10 CFR 73.55(g)(6)(i)(D))

Specific Guidance

The inspector(s) should verify that the licensee has addressed the compromise of access control devices and the unfavorable termination of employees who have access to access control devices to ensure that access to these controlled areas or systems remains controlled. The specific actions to ensure access control is maintained should be stated in implementing procedures to ensure that the members of the security organization responsible for these actions remain aware of their responsibilities and associated requirements. Actions to ensure access control is maintained should be

conducted in a timely fashion which should also be stated in the licensee implementing procedures.

f. Verify the licensee has implemented a numbered photo identification badge system for all personnel who are authorized unescorted access to the PA. (10 CFR 73.55(g)(6)(ii))

Specific Guidance

No inspection guidance.

g. Verify that personnel granted escorted access to the PA have their identity confirmed through physical presentation of a recognized identification card (local, state, federal government issued) that includes a photo or the physical characteristics of the individual; are badged to indicate that an escort is required; register his or her name, date, time, purpose of visit, employment affiliation, citizenship, and name of the individual to be visited before being escorted into the PA; and that the licensee maintains records of the escorted access retained for 3 years. (10 CFR 73.55(g)(7)(i) and 10 CFR 73.55(q)(2))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's security plans and implementing procedures pertaining to visitor registration and processing for escorted access into the PA to ensure that the licensee establishes and implements its process in accordance with the regulations. The inspector(s) should request that the licensee provide a copy of the licensee's visitor log or print a copy of inputs from an electronic database or allow the inspector(s) to view the electronic database to ensure all required information is obtained and recorded. If possible, the inspector(s) should observe the licensee process a visitor for escorted access into the PA or cause the licensee to perform a mock visitor registration process to ensure the elements as identified in this inspection requirement are performed.

h. Verify that neither the access control equipment (i.e., card reading devices, biometric devices, etc.), nor the access control measures at the PA personnel access control points allow an individual to enter or re-enter the PA without being identified, authorized, and searched prior to entry or re-entry. (10 CFR 73.55(g))

Specific Guidance

The inspector(s) should observe the design of the access control area to include physical barriers to ensure that the design of this area does not allow exit and re-entry into the PA without being subjected to the search process. If applicable, the inspector(s) should also observe a test of access control equipment at these portals to verify that attempts at re-entry without logging out are detected by alarms or notifications and that the access control equipment does not allow entry upon detection of attempted re-entry without logging out. Other measures that the licensee may be implementing, such as badge issuance and retrieval processes, personnel identification verifications (confirm the individuals true ID) when biometrics or similar is either out of service or not being used e.g., PA portal that doesn't have biometrics or similar, etc., should also be observed to ensure that the measures implemented provide controls that prevent the unauthorized bypass of the search process and access control equipment.

i. Verify the licensee provides an escort to all visitors at all times while inside the PA. (10 CFR 73.55(g)(7)(i)(E))

Specific Guidance

No inspection guidance.

j. Verify the licensee's visitor to escort ratios for the PA are implemented as described in its security plans. (10 CFR 73.55(g)(8)(v))

Specific Guidance

No inspection guidance.

k. Verify the licensee has established access control portals (personnel, material, and vehicle) outside of, or concurrent with, the physical barrier system (OCA and PA) through which it controls access. (10 CFR 73.55(g)(1)(i)(A))

Specific Guidance

No inspection guidance.

l. Verify the licensee has equipped access control portals with locking devices, intrusion detection equipment, and surveillance equipment consistent with the intended function. (10 CFR 73.55(g)(1)(i)(B))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's security plans and implementing procedures to identify the type of access control equipment being employed at each access control portal (personnel, material, and vehicle) and how it is being implemented to provide access control. The inspector(s) should verify through the observation of equipment operation and use that the locking devices, intrusion detection equipment, and surveillance equipment at all access control portals provide the protection required by regulation and as identified in the licensee's security plans and implementing procedures.

m. Verify the licensee implements and maintains measures, as necessary, to protect the badging process. (10 CFR 73.55(g)(1)(i)(C))

Specific Guidance

When inspecting the protection of the badging process, the inspector(s) should review the site security plans and associated implementing procedures to determine the locations the licensee has designated for production of picture badges and associated terminals that control the assignment of authorized access to electronic access control devices such as badges. The review of the security plans and implementing procedures should also provide the physical protection measures implemented at these locations to protect the badging process. All locations that possess the capabilities to produce picture badges and assign authorized access to the badges or other electronic access control devices should be inspected. The inspector(s) should physically verify, through observation, that these areas are supervised and controlled through methodologies that prohibit the surreptitious production of picture badges and manipulation of the access

control system to assign authorized access to electronic access control devices such as picture badges.

02.04 Controlling Access to Information

Verify the licensee, certificate holder, or applicant 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 10 CFR 73.21(b)(2))

Specific Guidance

For the inspection of this requirement, the inspector(s) should verify that the licensee has developed a program to address the control, protection, and designation of safeguards information, and that the implementing measures are documented in procedures.

The inspector(s) should review the licensee's implementing procedures for the control, protection, and designation of SGI to verify that the licensee 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 licensee provide a listing of personnel who have been authorized access to SGI and query licensee security management pertaining to the job description of these personnel which requires that they maintain access to SGI.

The inspector(s) should request that the licensee 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 licensee uses for the protection of SGI to the criteria in 10 CFR 73.2, “Definitions,” to ensure that the containers provide the required level of protection.

02.05 Security Equipment

a. Verify the licensee has developed testing and maintenance procedures for all security equipment identified as a component of the licensee’s physical protection program and protective strategy in accordance with the security plans and implementing procedures. (10 CFR 73.55(c)(7) and 10 CFR 73.55(n))

Specific Guidance

The inspector(s) should review the licensee’s security plans and implementing procedures for equipment maintenance and testing. This review should be conducted to determine that testing is performance-based, challenges the capabilities of the equipment, and is in accordance with the security plans and associated implementing procedures. The inspector(s) should also verify that the licensee’s testing and maintenance procedures are in accordance with the manufacturers’ design specifications for system application and conform to manufacturers’ recommendations for testing and maintenance.

The inspector(s) should confirm that the procedures describe testing that adequately challenges the equipment as it is presently installed and configured and for all functions it is required to perform. The licensee's testing procedures should also be compared to the applicable area of the licensee's security plans to ensure the testing procedures are consistent with the intended function of the equipment and that the testing performed does not reduce the effectiveness of the licensee's security plans.

b. Verify the perimeter intrusion detection system (IDS) and assessment equipment the licensee employs in support of its physical protection program and protective strategy is being maintained in accordance with the licensee's maintenance procedures to ensure operability and reliability. (10 CFR 73.55(n)(1))

Specific Guidance

For this inspection requirement, the inspector(s) should verify that the PA perimeter IDS, to include any intrusion detection devices that are employed to detect unauthorized entry into the PA (e.g., devices affixed to unattended openings that intersect a security boundary, etc.), are included in the licensee's maintenance program and are subject to a periodic or cyclic maintenance schedule. Additionally, if the licensee has a required Early Warning System (EWS), based on their site-specific analysis, the inspector(s) should verify that the EWS is also included in the licensee's maintenance program and is subject to a periodic or cyclic maintenance schedule. The inspector(s) should also review maintenance reports or logs to ensure that the maintenance performed on these systems is documented and meets the periodicity requirements and required maintenance activities established within licensee maintenance program procedures and manufacturers' recommendations. For additional guidance regarding EWS implementation see NRC Report on Interaction 2012-02, "Security Owner Controlled Area Barriers and IDS" (ADAMS Accession Number ML15323A379) and NRC Letter to the Industry, "The U.S. Nuclear Regulatory Commission Inspection Approach Related to Industry Implementation of Early Warning Systems," (ML16060A225).

c. Verify, through observation of testing activities, that the licensee's IDS detects attempted or actual penetration of the PA perimeter barrier before completed penetration and is tested in accordance with regulations and the licensee's testing procedures. (10 CFR 73.55(e)(7)(i)(B), 10 CFR 73.55(i) and 10 CFR 73.55(n))

Specific Guidance

For testing of the perimeter IDS, the inspector(s) should verify, through the observation of testing conducted by members of the security organization or NRC contractors, that the IDS is operating as intended and is capable of detecting attempted or actual penetration of the protected area barrier (PAB) prior to completed penetration of the barrier. If the licensee employs other intrusion detection devices in the OCA to detect unauthorized entry into the PA (e.g., devices affixed to unattended openings that intersect a security boundary, required EWS, etc.), the inspector(s) should also observe testing of these devices to verify their functionality under this inspection requirement and that testing is conducted in accordance with licensee testing procedures and manufacturers specifications to ensure acceptable system performance. For additional guidance regarding EWS implementation see NRC Report on Interaction 2012-02, "Security Owner Controlled Area Barriers and IDS" (ML15323A379) and NRC Letter to the Industry, "The U.S. Nuclear Regulatory Commission Inspection Approach Related to Industry Implementation of Early Warning Systems," (ML16060A225).

For perimeter IDS testing, the inspector(s) should select no less than three, and no more than six locations (zones) of the system for testing. The inspector(s) should observe testing activities conducted at each zone selected and cause the test subjects to conduct approaches at three locations within each zone (areas determined to possess potential vulnerabilities while ensuring ample zone coverage).

Each of the three locations selected within each zone should be tested using defeat methods applicable to the type and configuration of the system being tested. System and device support beams or poles to which system sensors are anchored or affixed should also be included in the test. Testing at these support or anchor locations should be conducted to ensure the system provides detection at these locations and that these locations cannot be bypassed without detection. Each test approach should be performed until the alarm is received in the alarm station and is communicated to the test subject. The licensee should be able to demonstrate that if an area seems susceptible to jumping that the zone in question cannot be circumvented through jumping. The licensee can use a device such as an aluminum ball, 12 inches in diameter, being passed over the zone to conduct simulated jump testing. Testing of IDS should be conducted with one physical security inspector(s) stationed in the central alarm station (CAS) to verify that alarms annunciate concurrently in both alarm stations, audibly and visually, and that there is an indication of the type and location of the alarm and that alarm station assessment equipment provides video images from which assessment can be made and provide real-time and play-back recorded video images before and after each alarm annunciation. A second physical security inspector(s) should observe licensee personnel perform the intrusion tests at the PA perimeter.

See Regulatory Guide 5.44, “Perimeter Intrusion Alarm Systems,” for further guidance on perimeter intrusion detection testing. The testing of these devices must be conducted at least once every 7 days and as further stated in licensee security plans and implementing procedures.

d. Verify through observation of testing activities, that alarm devices are tamper-indicating and self-checking, including transmission lines to their respective annunciators and junction boxes and that these tests are conducted in accordance with regulations and licensee testing procedures. (10 CFR 73.55(i)(3)(iv) and 10 CFR73.55(n))

Specific Guidance

To conduct the inspection of the perimeter IDS to determine that the system possesses the capability to indicate system tampering and system or component failure, the inspector(s) should review the design specifications and manufacturers’ technical documentation for the perimeter IDS to determine that the system possesses the capability to indicate system tampering and system or component failure. The inspector(s) should also verify that the licensee’s testing procedures are in accordance with the manufacturers’ specifications for testing this specific function of these systems to ensure the testing demonstrates acceptable system performance. The licensee’s testing procedures should also be compared to the perimeter intrusion detection objectives identified in the licensee’s security plans to ensure the procedures do not reduce the effectiveness of the licensee’s security plans. The inspector(s) should then physically verify, through observation of testing conducted by members of the security organization, that when system components are physically manipulated (in accordance with testing procedures) that the system provides an indication of tampering and/or

component failure on the alarm station console. Inspector(s) should inspect a sample of the licensee's perimeter intrusion detection devices to complete this inspection requirement, but no more than two exterior devices employed within the system should be subjected to this testing.

e. Verify that PA assessment capability provides for the assessment of detected activity at the PA perimeter and the initiation of timely response. (10 CFR 72.212(b)(9)(iv) and 10 CFR 73.55(i)(3))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's security plans and associated implementing procedures to determine the specific methodology being implemented for assessment at the licensee's PA perimeter. Licensees may implement electronic technologies (e.g., closed circuit television) or direct surveillance conducted by a member of the licensee's security organization via patrol to satisfy this requirement; this guidance only applies to ISFSIs not in the same PA as the reactor.

f. Verify through observation of testing activities, that video assessment assets at the PA perimeter provide a visual display from which assessment can be made and provide real-time and play-back recorded video images of detected activities before and after each alarm annunciation and that these devices are tested in accordance with regulations and the licensee's testing procedures. (10 CFR 73.55(e)(7)(i)(C), 10 CFR 73.55(i)(3)(ii), and 10 CFR 73.55(n))

Specific Guidance

The inspection of PA perimeter assessment devices should be conducted in conjunction with and during the perimeter IDS testing. If the licensee employs surveillance devices in the OCA to prevent unauthorized entry into the PA (i.e., devices that are specifically used for the surveillance of unattended openings that intersect a security boundary, required EWS, etc.), the inspector(s) should also observe testing of these devices to verify their functionality under this inspection requirement and that these systems are tested in accordance with licensee testing procedures. For PA perimeter assessment equipment, the inspector(s) should verify, through the observation of testing conducted by members of the security organization that the perimeter video assessment assets perform as designed and provide real-time and play-back recorded video images of detected activities before and after each alarm annunciation. The inspector(s) located in the CAS should verify that the video image recording equipment provides a clear video image from which an assessment can be made both in real-time and play-back mode. The inspector(s) in the CAS should observe the video monitors associated with the perimeter assessment assets during testing and query the alarm station operator pertaining to the images being provided to ensure assessment capabilities during the test approaches. The play-back recorded video image of alarm annunciations should also be reviewed and verified. See Regulatory Guide 5.44, "Perimeter Intrusion Alarm Systems," for further guidance on perimeter video assessment equipment testing. The testing of these devices must be conducted at least once every 7 days and as further stated in licensee security plans and implementing procedures.

g. Verify through observation of testing activities or through testing and maintenance record review that the intrusion detection system provides an automatic indication when the alarm system or a component of the system fails or when the system is operating on back-up power and that testing of this function is conducted in accordance with regulations and the licensee testing procedures. (10 CFR 73.55(i)(3)(v) and 10 CFR 73.55(n))

Specific Guidance

The inspector(s) should verify during the conduct of perimeter IDS tamper testing and the testing of the uninterruptible power supply (UPS) or through testing and maintenance record review that the alarm station console receives automatic indications when components are out of service and when the system is operating on backup power.

h. Verify (as applicable) that where building walls or roofs comprise a portion of the PA perimeter barrier where the licensee has not established an isolation zone, that the licensee has implemented detection and assessment methodologies and physical barriers that meet the requirements of 10 CFR 73.55 and that this area is described in the security plans. (10 CFR 73.55(e)(8)(iv))

Specific Guidance

The inspection of this requirement should be conducted in conjunction with perimeter intrusion detection and assessment system testing. The inspector(s) should physically verify, through observation, that these areas are equipped with intrusion detection and assessment equipment that cover the entire area of the wall of the building and/or the roof that is a portion of the PAB where there is no isolation zone. The inspector(s) should also verify that the equipment in these areas provides detection and assessment in accordance with the regulations and licensee security plans and implementing procedures. For additional guidance regarding implementation where buildings, walls or roofs that comprise a portion of the PA barrier see SFAQ 17-01 “Intrusion Detection Capability for Portions of a Protected Area Boundary Formed be a Building Interior Structure”. (ML17339A061)

i. Verify that internal detection and assessment equipment the licensee employs in support of its physical protection program and protective strategy is being maintained in accordance with the licensee maintenance procedures to ensure operability and reliability. (10 CFR 73.55(n)(1))

Specific Guidance

For the inspection of this requirement the inspector(s) should verify that the internal intrusion detection and assessment equipment the licensee employs in support of its physical protection program and protective strategy is included in the licensee’s maintenance program and is subject to a periodic or cyclic maintenance schedule.

The inspector(s) should also review maintenance reports or logs to ensure that the maintenance performed on the system is documented and meets the periodicity requirements and required maintenance activities established within licensee maintenance program procedures and manufacturers’ recommendations.

j. Verify that alarm station console equipment the licensee employs in support of its physical protection program and protective strategy is being maintained in accordance with the licensee maintenance procedures to ensure operability and reliability. (10 CFR 73.55(n)(1))

Specific Guidance

For the inspection of this requirement, the inspector(s) should verify that the alarm station console equipment that the licensee employs in support of its physical protection program and protective strategy is included in the licensee's maintenance program and is subject to a periodic or cyclic maintenance schedule. The inspector(s) should also review maintenance reports or logs to ensure that the maintenance performed on the system is documented and meets the periodicity requirements and required maintenance activities established within licensee maintenance program procedures and manufacturers' recommendations.

k. Verify there are no activities performed within the alarm stations which would interfere with the alarm station operators' ability to execute the detection and assessment of alarms, the initiation and coordination of an adequate response to alarms, the summoning of off-site assistance, and their ability to provide command and control. (10 CFR 73.55(i)(4)(ii)(C))

Specific Guidance

When inspecting this requirement, the inspector(s) should review the licensee's security plans and implementing procedures to determine if there are any other activities conducted within or from the alarm stations. The inspector(s) should then observe these additional activities within the alarm station to evaluate whether these activities interfere with the alarm station operator's ability to perform alarm station duties and responsibilities. Alarm station operators must be able to: (1) detect and assess alarms; (2) initiate and coordinate response; (3) summon offsite assistance; and (4) provide command and control without interference.

l. Verify the following configuration requirements for the CAS: (1) is located inside a PA; (2) interior must not be visible from the PA perimeter; and (3) is constructed to be bullet resisting; (4) is designated as a VA (as appropriate) (10 CFR 73.55(e)(5), 10 CFR 73.55(e)(9), and 10 CFR 73.55(i)(4)(ii)(A))

Specific Guidance

If applicable, depending on the site configuration the CAS might not be located in a VA. An ISFSI is a spent fuel storage facility, and the licensee is no longer authorized to operate, or the reactor core has been removed, therefore there are no VAs at an ISFSI facility. This does not apply to a co-located ISFSI.

m. Verify through observation of testing activities, that CAS maintains continuous communication capabilities with each on-duty security force member and that the testing of this function is conducted in accordance with regulations and licensee testing procedures. (10 CFR 73.55(j)(3), 10 CFR 73.55(j)(4) and 10 CFR 73.55(n)(4))

Specific Guidance

For the testing of communication devices, the inspector(s) should verify through observation of testing (communication checks), that all communication equipment used for communicating with on-duty security force members operates as designed. The testing should include multiple radio checks with the different members of the security organization deployed in the field of duty. Backup communication devices, identified by the licensee in security plans and implementing procedures, for communication with the security force should also be tested (i.e., radios, station intercom systems, etc.). The inspector(s) should observe communication checks conducted from each alarm station during the conduct of testing under this requirement. The inspector(s) should verify that the testing of these communication devices is conducted at least once per shift (at the beginning of shift) and further as stated in security plans and implementing procedures.

n. Verify the licensee has a process in place to maintain the integrity of all of its physical barriers, including OCA and PA barriers. (10 CFR 73.55(i)(5)(ii), (iv), and 10 CFR 73.55(n)(1))

Specific Guidance

For the inspection of this requirement, the inspector(s) should verify that all physical barriers that the licensee employs in support of its physical protection program and protective strategy are periodically inspected for integrity and as applicable included in the licensee's maintenance program and subjected to a periodic or cyclic maintenance schedule. If applicable, the inspector(s) should also review maintenance reports or logs to ensure that the maintenance performed on physical barriers system(s) is documented and meets the periodicity requirements and required maintenance activities established within licensee maintenance program procedures and manufacturers' recommendations.

o. Verify the operation of active vehicle barrier systems (AVBS) are periodically checked through testing in accordance with licensee testing procedures. (10 CFR 73.55(e)(10)(i)(B) and 10 CFR 73.55(n)(1))

Specific Guidance

When inspecting this requirement, the inspector(s) may review the licensee's testing procedures and records to verify that the licensee has established and implements a method to periodically check the operation of the system in accordance with regulations. If the inspector(s) observes a test of the AVBS, the inspector(s) should familiarize themselves with the licensee's active vehicle barrier testing procedures to ensure that the testing of active vehicle barriers, as observed, is consistent with what is identified in procedures. The inspector(s) should also verify that the licensee's testing procedures are in accordance with the manufacturers' specifications for these systems to ensure testing for these systems demonstrates acceptable system performance. The licensee's testing procedures should also be compared to the vehicle control measures which are identified in the licensee's security plans to ensure the procedures do not reduce the effectiveness of the licensee's security plans. The inspector(s) should verify, through the observation of testing conducted by members of the security organization that the active vehicle barrier(s) operate (in all modes of operation) as designed. The inspector(s) should observe testing activities conducted at each control panel associated with the barrier to ensure overall system operability.

p. Verify through the observation of testing activities, that isolation zones are designed and of sufficient size to permit observation and assessment of activities on either side of the PA barrier. (10 CFR 73.55(e)(7))

Specific Guidance

The inspection of this requirement should be conducted and can be satisfied in conjunction with perimeter intrusion detection and assessment system testing. The inspector(s) should ensure that observation and assessment can be accomplished on both the external and internal sides of the PA barrier.

q. Verify the licensee's testing and evaluation procedures are consistent with the manufacturers' design characteristics, performance specifications, and testing recommendations to ensure the equipment is being tested and evaluated to meet acceptance criteria. (10 CFR 73.55(n)(1)(ii))

Specific Guidance

For this requirement, the inspector(s) should ensure that licensee procedures for evaluation and analysis include following the manufacturers' recommendations for appropriate application and implementation of the subsystem or component, the manufacturers' testing recommendations, and acceptance criteria.

r. Verify that illumination within the isolation zones and external areas of the PA is being maintained and/or augmented by low-light technology in accordance with regulatory requirements to support assessment and response activities and that this equipment is tested in accordance with regulations and licensee testing procedures. (10 CFR 73.55(i)(6) and 10 CFR 73.55(n))

Specific Guidance

For the inspection of this requirement the inspector(s) should review licensee security plans and implementing procedures to determine how the licensee provides the illumination necessary to satisfy isolation zone and external PA assessment requirements. The inspector(s) may review licensee testing records to verify that testing of these assets during the hours of darkness has consistently enabled members of the security organization to observe and assess activities in isolation zones and external areas of the PA. The inspector(s) should physically verify a sample of the illumination (a minimum of four tested areas) provided in isolation zones and external areas of the PA during the hours of darkness. For testing during the hours of darkness, the inspector(s) should select areas (at least four) that appear to have insufficient illumination. The inspector(s) should verify through the observation of testing by a member of the security organization with a light meter that the illumination assets in the isolation zone and the appropriate external areas of the PA provides at least 0.2 foot candles of illumination measured horizontally at ground level in the tested area. If the licensee utilizes other technology in conjunction with its illumination to provide assessment capabilities during the hours of darkness, then the inspector(s) should verify that this equipment, when used in conjunction with existing illumination, provides the ability to conduct assessment of detected activities in accordance with 10 CFR 73.55(i), licensee security plans, and implementing procedures.

s. Verify that a record of all alarm annunciations is maintained which includes the cause of the alarm and the final disposition of the alarm as determined by the licensee's security force. (10 CFR 73.55(i)(4)(ii)(H))

Specific Guidance

The inspector(s) should review the manufacturers' technical documentation for the alarm station console to determine that the system possesses the capability to record all alarm annunciations. To complete the inspection of this requirement, the inspector(s) should inspect both the central and secondary alarm station for these capabilities and cause the alarm station operators to display or print a sample of alarm annunciations received during intrusion detection system testing. The inspector(s) should also verify that the alarm stations possess the capability to record the cause of the alarms and the disposition of the alarms through electronic or manual means.

t. Verify the compensatory measures that the licensee is implementing to compensate for degraded or inoperable equipment, systems, and components meet all regulatory requirements. (10 CFR 73.55(o))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's security plans and implementing procedures to verify that the licensee has appropriately implemented compensatory measures for degraded or inoperable equipment, systems, and components. Compensatory measures are required to meet the following criteria:

Provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, systems, or components.

Were implemented within the specific timeframes necessary to meet regulatory requirements and are described in the security plans.

The inspector(s) should interview cognizant licensee security staff to identify compensatory measures that are currently being implemented. This information can also be found in security shift blotters or logs. Additionally, licensee technical staff may be interviewed to identify degraded or inoperable equipment that would require compensatory measures. The inspector(s) should review log entries and/or shift blotters to verify time of failure and time of compensatory measure implementation. The inspector(s) should evaluate the compensatory measures to ensure they provide level of protection that was equivalent to that which was provided by the degraded or inoperable system and that the compensatory measure was implemented in a timeframe consistent with licensee security plans and implementing procedures. Additionally, a review of log entries and or shift blotters can be verified as well as the licensee's corrective action program (CAP). The CAP should identify when the degradation or failure was identified.

02.06 Local Law Enforcement Agency (LLEA)

Verify the licensee has a documented agreement with applicable LLEA to include estimated response times and capabilities. (10 CFR 73.55(k)(9))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the documented liaison that the licensee has established with LLEA (local, state, federal). The liaison should be in the form of a written document (i.e., letter, agreement, memorandum of understanding, etc.) that demonstrates that the licensee has requested the assistance of these agencies to support its security force with contingency events. The inspector(s) should verify the licensee's established law enforcement liaison to the extent documented in security plans and implementing procedures.

02.07 Weapons Maintenance

a. Verify (if applicable) that the licensee has established and implements measures for the control and accountability of all assigned firearms and ammunition.

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's physical security plan, firearms and ammunition control and accountability procedures. The inspector(s) should verify, through a review of records and through observation, that firearms control and accountability measures are being implemented in accordance with physical security plan, licensee procedures and that these measures restrict unauthorized access to firearms and ammunition. Accountability measures should be conducted at a periodicity that would provide a timely indication that a firearm is missing or has an unknown disposition.

b. Verify (if applicable) that the licensee documents activities associated with its firearms maintenance program.

Specific Guidance

The inspector(s) should review the licensee's physical security plan and weapons maintenance program procedures. The inspector(s) should verify, through a review of records, that firearms maintenance documentation is maintained, which should include a description of the type of maintenance, repair or modification completed, the date completed, and the individual who performed the activity. Firearms shipping documentation should also be maintained, as this is a manner in which the licensee can account for firearms that are in transit for maintenance, repair, or modifications.

02.08 Reviews

a. Events and Logs. Review and evaluate licensee event reports and safeguards log entries for the previous 12 months, or since the last inspection. (10 CFR 73.55(b)(10) and 10 CFR 73.71)

b. Security Program Reviews. Verify that the licensee is conducting security program reviews in accordance with 10 CFR 73.55(m).

c. Identification and Resolution of Problems. Verify that the licensee is identifying issues related to the security program at an appropriate threshold and entering them in the corrective action program. Verify that the licensee has appropriately resolved the issues

regarding regulatory requirements for a selected sample of problems associated with the security program. (10 CFR 73.55(b)(10))

Specific Guidance

Before the inspection, the inspector(s) should review and evaluate licensee event reports and safeguards log entries, since at least the last inspection, that are associated with the access control program. If discrepancies or deficiencies are identified during this review, the inspector(s) should follow up as necessary.

For the inspection of this requirement, the inspector(s) should review the documented results of the security program reviews or audits performed by the licensee to ensure the continued effectiveness of its security program.

The inspector(s) should ensure that the reviews have been conducted in accordance with the requirements of 10 CFR 73.55(m). The inspector(s) should also request that the licensee provide a copy of the report that was developed and provided to licensee management for review. The inspector(s) should review the report to identify any findings that were identified via the review or audit to ensure the findings were entered in the licensee's corrective action program.

02.09 Specific License Requirements and Guidance

Requirements of 10 CFR 72 Subpart H and 10 CFR 73.51 are applicable for the physical protection of spent nuclear fuel (SNF) and power reactor-related GTCC waste stored under a specific ISFSI license issued pursuant to 10 CFR 72.40. Through verification of the inspection requirements within this IP, inspector(s) shall verify or determine that the licensee's physical protection program is designed and implemented to meet the general performance objective of 10 CFR 73.51(b); specific requirements under 10 CFR 72.180, 72.182, 72.184, and 72.186 of Subpart H; and site-specific security orders (e.g., interim compensatory measures and additional security measures). Inspector(s) should note that ICMs and ASMs are two different documents that encompass the same requirements. Licensees who had an existing ISFSI prior to September 2007 were issued the ICMs and licensees who built an ISFSI after September 2007 were issued the ASMs.

a. Verify that SNF and power reactor-related GTCC waste is stored only within a PA. (10 CFR 73.51(b)(2)(i)) and (10 CFR 73.51(d)(1))

Specific Guidance

To inspect this requirement the inspector(s) should observe a sample of a few physical barriers (surrounding the PA to which access is controlled) that the licensee has established and installed to verify the integrity of the barriers (ability to perform their intended function) and that the barriers are designed and constructed of materials in accordance with10 CFR 73.2, Definitions, "Physical Barriers." For the PA perimeter barrier, the inspector(s) should take sample measurements of the barrier in any locations that appear to be less than the prescribed height and verify that any opening in the barrier is secured and monitored in accordance with the regulation. If building walls comprise a portion of the PA barrier, the inspector(s) should verify that the building (barrier) height and material is in accordance with 10 CFR 73.2, Definitions, "Physical Barriers."

b. Verify that only individuals who are authorized to enter the PA are granted access to the PA. (10 CFR 73.51(b)(2)(ii))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review a sample (up to five) of the licensee's access authorization program records ensuring sufficient information on which to base an initial determination to grant a person unescorted access. The total accumulation of information within those records about the individual must be the basis for the access determination for each record sample.

c. Verify the licensee is in compliance with site specific security orders (e.g., additional security measures) for access authorization and fingerprinting; a log of authorized individuals is required by 10 CFR 73.51(d)(13)(i).

Specific Guidance

No inspection guidance

d. Verify the licensee can detect and assess penetrations through the isolation zone (IZ). (10 CFR 73.51(b)(2)(iii) and 10 CFR 73.51(d)(3))

Specific Guidance

For the inspection of this requirement, the inspector(s) should observe that all physical barriers that the licensee employs in support of its physical protection program and protective strategy are periodically inspected for integrity, and as applicable, are included in the licensee's maintenance program and subject to a periodic or cyclic maintenance schedule. If applicable, the inspector(s) should also review maintenance reports or logs. For testing of the perimeter intrusion detection system (IDS) the inspector(s) should verify, through the observation of testing conducted by members of the security organization, that the IDS is operating as intended and is capable of detecting penetrations through the IZ. The inspector(s) should observe that the licensee's perimeter assessment capabilities provide for timely assessment of intrusion alarms at the PA perimeter to ensure the initiation of a timely response.

If the licensee employs other intrusion detection devices in the OCA to detect unauthorized entry into PA, the inspector(s) should also observe testing of these devices to verify their functionality and that testing is conducted in accordance with licensee testing procedures. Each zone selected should be tested by the licensee's personnel using methods applicable to the type and configuration of the system being tested. System and device support beams or poles to which system sensors are anchored or affixed should also be included in the test. Each test approach should be performed until the alarm is received in the alarm station and is communicated to the test subject.

e. Verify the licensee can provide timely communication to the designated response force whenever necessary. (10 CFR 73.51(b)(2)(iv))

Specific Guidance

For the inspection of this requirement, the inspector(s) should observe checks of communication equipment and verify that all equipment used for communicating with the

designated response force or local law enforcement agency (LLEA) operates as designed.

f. Verify the physical protection system is designed to protect against loss of control of the facility that could be sufficient to cause a radiation exposure exceeding the dose as described in 10 CFR 72.106(b). (10 CFR 73.51(b)(3))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review and verify that the licensee security plans have established measures to maintain an onsite physical protection program. Licensee security plans should discuss and identify members of the security organization and their duties and responsibilities. Additionally, the inspector(s) should verify that licensee implementing procedures ensure that all members of the security organization remain aware of their responsibilities and associated requirements. Lastly, inspector(s) will verify that all security systems and equipment are serviceable, in operation, and functioning properly.

g. Verify the licensee has retained a copy of the physical protection plan for a period of 3 years or until termination of the license. (10 CFR 73.51(c))

Specific Guidance

No inspection guidance.

h. Verify the licensee complies with the provisions for physical protection systems, components, and procedures that meet the performance objectives of 10 CFR 73.51(b)(1). (10 CFR 73.51(b)(2) and 10 CFR 73.51(d))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review records and observe demonstrations. The licensee should be able to show that all security equipment that is identified as a component of the physical protection program has been tested to ensure the equipment remains operable and maintains the capability to perform its intended function. Manufacturers' recommendations and specifications for equipment maintenance, testing (includes both routine/periodic and acceptance testing) and calibration are important elements in ensuring the security system maintains the capability to perform its intended function. The inspector(s) should verify that the licensee has incorporated and is adhering to manufacturers' recommendations and specifications to ensure the equipment can perform as designed.

The environment in which security equipment is employed is also an important factor in ensuring the capability of security equipment to perform as intended and should also be addressed in accordance with the manufacturers' recommendations and specifications.

For certain physical protection systems, sensitivity settings may have to be adjusted to accommodate certain environmental conditions (e.g., consistent wind, moisture or rain, fog, high voltage areas, radio frequency interference, etc.); however, these systems must maintain the capability to perform their intended function and meet the specific acceptance criteria that has been established in NRC regulations, regulatory guidance documents, and by the manufacturer of the systems.

i. Verify the licensee provides illumination sufficient to permit adequate assessment of unauthorized penetrations of or activities within the PA. (10 CFR 73.51(d)(2))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review licensee security plans and implementing procedures to determine how the licensee provides the illumination necessary to satisfy IZ and PA assessment requirements. The inspector(s) may review licensee testing records to verify that testing of these assets during the hours of darkness had consistently enabled members of the security organization to observe and assess activities in IZs and external areas of the PA. If the licensee utilizes other technology in conjunction with its illumination to provide assessment capabilities during the hours of darkness, then the inspector(s) should verify that this equipment, when used in conjunction with existing illumination, provides the ability to conduct assessment of detected activities.

j. Verify the licensee's perimeter of the PA allows for continual surveillance and is protected by an active intrusion alarm system that is capable of detecting penetrations through the IZ and that is monitored in a continually staffed primary alarm station and in one additional continually staffed location. (10 CFR 73.51(d)(3))

Specific Guidance

The inspection of PA perimeter assessment devices should be conducted in conjunction with and during the perimeter IDS testing. For PA perimeter assessment equipment, the inspector(s) should verify through the observation of testing conducted by members of the security organization.

k. Verify the primary alarm station is located within the PA and it has bullet-resisting walls, doors, ceiling and floor, and the interior of the station is not visible from outside the PA. (10 CFR 73.51(d)(3))

Specific Guidance

No inspection guidance.

l. Verify the licensee conducts an assessment of all alarms in a timely means. The redundant location need only provide a summary indication that an alarm has been generated. (10 CFR 73.51(d)(3))

Specific Guidance

No inspection guidance.

m. Verify the licensee's PA is monitored by daily random patrols. (10 CFR 73.51(d)(4); a log of all patrols is required by 73.51(d)(13)(iii)).

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the security plan, implementing procedures, post orders, and logs of random security patrols of external and internal areas of the PA. These patrols should be conducted to detect the presence of unauthorized personnel, materials, vehicles, or activities and should include

observations and verifications of physical protection program equipment and measures to ensure the integrity of the equipment and the proper implementation of security measures.

n. Verify the licensee's security organization has written procedures that provides for sufficient personnel per shift to ensure the monitoring of detection systems and the conduct of surveillance, assessment, access control, and communications to assure adequate response. Members of the security organization must be trained, equipped, qualified, and requalified to perform assigned job duties in accordance with Appendix B to Part 73, sections I.A, (1)(a) and (b), B(1)(a), and the applicable portions of section II. (10 CFR 73.51(d)(5))

Specific Guidance

For the inspection of this requirement, the inspector(s) should verify that the licensee has screened, trained, and qualified all members of the security organization required to implement any part of the physical protection program. The inspector(s) should review a sample of employment screening records and/or training records that document each individual was screened, trained, and qualified to perform duties. Additionally, the inspector(s) should verify that the individuals have access to any and all equipment required to perform the duties associated with their position.

o. Verify the licensee has a documented liaison with a designated response force or LLEA to permit a timely response to unauthorized penetration or activities. (10 CFR 73.51(d)(6))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the documented liaison that the licensee has established with LLEA (local, State, Federal). The liaison should be in the form of a written document (i.e., letter, agreement, memorandum of understanding, etc.) that demonstrates that the licensee has requested the assistance of these agencies to support its security force with contingency events. The inspector(s) should verify the licensee's established law enforcement liaison to the extent documented in security plans and implementing procedures.

p. Verify the licensee has a personnel identification system and a controlled lock system that limits access to only authorized individuals. (10 CFR 73.51(d)(7))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review the licensee's security plan and implementing procedures to identify security systems for which the licensee controls access. The security systems that should have access control measures associated with them could be areas such as alarm stations, access badging terminals, or secondary power supplies for alarm annunciation equipment and communications systems that are required by regulation or through the licensee's security plan and implementing procedures. Access controls implemented by the licensee may include equipment or systems that are maintained in a locked area with the specific keys or key cards for entry to the area being controlled. Additionally, passwords that provide access to the functions of a security computer system(s) or an access badging terminal should also be controlled.

q. Verify the licensee has redundant communications capability between onsite security force members and designated response force or LLEA. (10 CFR 73.51(d)(8))

Specific Guidance

For the inspection of this requirement, the inspector(s) should review, through observation of testing, that the communication equipment operates as designed. The testing should include at least one communication check using each method of communication with LLEA. Backup communication devices, identified by the licensee in their security plans and implementing procedures, for communication with the security force should also be tested (i.e., radios, station intercom systems, etc.).

r. Verify all individuals, vehicles, and hand-carried packages entering the PA are checked for proper authorization and visually searched for explosives before entry. (10 CFR 73.51(d)(9))

Specific Guidance

For the inspection of this requirement, the inspector(s) should ensure that the licensee is implementing its access control program for personnel, materials, and vehicles in accordance with the regulatory requirements and any other applicable NRC requirements. When inspecting this requirement, the inspector(s) should review the licensee's procedures to verify that the licensee has established methods for granting access to personnel, materials, and vehicles into the PA.

s. Verify the licensee's written response procedures have been established and maintained for addressing unauthorized penetration of, or activities within, the PA. (10 CFR 73.51(d)(10))

Specific Guidance

For inspection of this requirement, the inspector(s) should familiarize themselves with relevant documentation pertaining to response which may include, but is not limited to, the licensee's security plans, site-specific and/or corporate implementing procedures, security post orders, and security program reviews and audits. The licensee's documentation should include how they comply with 10 CFR 73, Appendix C, Section II, B.(5), "Implementing Procedures." Copies of superseded material must be retained for 3 years after each change or until termination of the license.

t. Verify all the licensee's detection systems and supporting subsystems include a tamper indicating system with line supervision. The system, as well as surveillance/assessment and illumination systems, must be maintained in operable condition. (10 CFR 73.51(d)(11))

Specific Guidance

For this inspection requirement, the inspector(s) should review the design specifications and manufacturers' technical documentation for the perimeter IDS to determine that the system possesses the capability to indicate system component failure. The inspector(s) should verify that the licensee's testing procedures are in accordance with the manufacturers' specifications for testing this specific function of these systems to ensure the testing demonstrates acceptable system performance. The licensee's testing

procedures should also be compared to objectives identified in the licensee's security plans to verify that the procedures do not reduce the effectiveness of the licensee's security plans. The inspector(s) should then physically verify, through observation of testing conducted by members of the security organization, that when system components are physically manipulated (in accordance with licensee testing procedures) the system provides an indication of tampering and/or component failure. Inspector(s) should inspect a sample of the licensee's perimeter intrusion detection devices to complete this inspection requirement. Timely compensatory measures must be taken after discovery of inoperability, to assure that the effectiveness of the security system is not reduced. (10 CFR 73.51(d)(11))

u. Verify the licensee protects safeguards information against unauthorized disclosure.(10 CFR 73.21 and 10 CFR 73.22).

Specific Guidance

For the inspection of this requirement, the inspector(s) should verify that the licensee has developed a program to address the control, protection, and designation of safeguards information, and that the implementing measures are documented in procedures.

The inspector(s) should review the licensee's implementing procedures for the control, protection, and designation of SGI to verify that the licensee 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 licensee provide a listing of personnel who have been authorized access to SGI and query licensee security management pertaining to the job description of these personnel which requires that they maintain access to SGI.

The inspector(s) should request that the licensee 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 licensee 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.

v. Verify the licensee's physical protection program is reviewed once every 24 months by individuals independent of both physical protection program management and personnel who have direct responsibility for implementation of the physical protection program. The physical protection program review must include an evaluation of the effectiveness of the physical protection system and a verification of the liaison established with the designated response force or LLEA. (10 CFR 73.51(d)(12))

Specific Guidance

No inspection guidance.

w. Verify the licensee has retained the following documentation as a record for 3 years after the record is made or until termination of the license: a log of individuals granted access to the PA; screening records of members of the security organization; a log of all patrols;

a record of each alarm received, identifying the type of alarm, location, date, and time when received, and disposition of the alarm; and the physical protection program review reports. (10 CFR 73.51(d)(13)(i)(ii)(iii)(iv) and (v))

Specific Guidance

No inspection guidance.

x. Verify, in accordance with any applicable security requirements and/or security orders that the licensee has implemented measure and process for vehicle control measures into PAs.

Specific Guidance

For the inspection of this requirement, the inspector(s) should review site security plans and implementing procedures to verify the licensee has implemented vehicle control measures that may include the use of vehicle barriers, active and passive, along with any implementing procedures for processing vehicles into PAs.

y. Verify, in accordance with any applicable security requirements and/or security orders, that the licensee has implemented an insider mitigation program.

Specific Guidance

No inspection guidance.

z. Verify the licensee has developed off site response coordination with LLEA as applicable to physical security requirements and/or security orders.

Specific Guidance

For inspection of this requirement, the inspector(s) should familiarize themselves with relevant documentation pertaining to response which may include, but is not limited to, the licensee's security plans and any written agreements from off-site response agencies.

81311-03 PROCEDURE COMPLETION

This procedure is considered complete when all of the applicable inspection requirements listed within this procedure have been completed. There are 51 inspection requirements for a general license and 26 inspection requirements for a specific license.

81311-04 RESOURCE ESTIMATE

The resource estimate for the completion of this procedure consists of 16 hours for the inspection of a co-located ISFSI, at a reactor, and 24 hours for the inspection of a non co-located ISFSI, away from reactor. The frequency at which this inspection activity is to be conducted is triennially (once every 3 years).

81311-05 REFERENCES AND ASSOCIATED PUBLICATIONS

05.01 References.

Interim Compensatory Measures (ICMs) for Dry Spent Fuel Storage, October 16, 2002. SLES Reference No. NS106674

Additional Security Measures (ASMs) for the Physical Protection of Dry Independent Spent Fuel Storage Installations, September 28, 2007. SLES Reference No. NS106675

Additional Security Measures for Access Authorization and Fingerprinting at Independent Spent Fuel Storage Installations, December 19, 2007. SLES Reference No. NS107943

RG 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials," Revision 1, October 2016. (ML15357A411)

RG 5.44, "Perimeter Intrusion Alarm Systems," Revision 3, October 1997. (ML003739217)

RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities," March 2021. (ML17111A699)

RG 5.77, "Insider Mitigation Program," March 2009. (ML090721034)

RG 3.60, "Design of an Independent Spent Fuel Storage Installation (Dry Storage)," March 1987. (ML082681195)

IP 60858, "Away-From-Reactor ISFSI Inspection Guidance," November 12, 2020. (ML20294A520)

Inspection Manual Chapter 2690, "Inspection Program for Dry Storage of Spent Reactor Fuel at Independent Spent Fuel Storage Installations and for 10 CFR Part 71 Transportation Packaging's," December 15, 2020. (ML20338A192)

Enforcement Guidance Memorandum 04-002, "Guidance for Handling Security-Related Enforcement Documents," dated May 21, 2004. (ML040750434)

05.02 Associated Publications.

NUREG-1140, "A Regulatory Analysis on Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees, Final Report," January 1988. (ML062020791)

NUREG-1567, "Standard Review Plan for Spent Fuel Dry Storage Facilities," March 2000. (ML003686776)

PDC-TR-06-03, "U.S. Army Corps of Engineers Protective Design Center Technical Report. Vehicle Barrier Maintenance Guidance," February 24, 2007. (ML070590251)

END

Attachment 1 - Revision History for IP 81311, .

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	ML103440331 06/02/11 CN 11-009	First Issuance. Completed 4 year search for commitments and found none.	N/A	N/A
N/A	ML16337A045 08/25/17 CN 17-016	This IP was amended to separate the requirements associated with the types and locations of ISFSI's. Portion markings were added to the inspection document. This is a major re-write.	N/A	ML16337A043
N/A	ML18288A186 02/08/19 CN 19-006	A periodic review of this document was conducted to ensure consistency with other associated NRC Manual Chapters and IPs. Staff also corrected a few technical modifications that were missing in this document. Upon completion of a SUNSI review, the staff concluded that this document can be decontrolled. The staff has removed all portion markings.	N/A	ML18288A187
N/A	ML20265A169 10/06/20 CN 20-048	This revision was to apply administrative changes reflecting this document's applicability by removing IMC 2515C and 2561B	N/A	ML20265A175
N/A	ML21202A298 06/28/22 CN 22-014	This revision was to further clarify the applicability of requirements as they are to be applied to the different license holders of ISFSI's. Additionally, upon completion of a SUNSI review, the staff concluded that this document would remain decontrolled.	N/A	ML21202A303