**THIS PRELIMINARY PROPOSED RULE LANGUAGE AND ACCOMPANYING DISCUSSION IS BEING RELEASED TO SUPPORT INTERACTIONS WITH STAKEHOLDERS AND THE ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS). THIS LANGUAGE HAS NOT BEEN SUBJECT TO COMPLETE NRC MANAGEMENT OR LEGAL REVIEW, AND ITS CONTENTS SHOULD NOT BE INTERPRETED AS OFFICIAL AGENCY POSITIONS. THE NRC STAFF PLANS TO CONTINUE WORKING ON THE CONCEPTS AND DETAILS PROVIDED IN THIS DOCUMENT AND WILL CONTINUE TO PROVIDE OPPORTUNITIES FOR PUBLIC PARTICIPATION AS PART OF THE RULEMAKING ACTIVITIES.**

**THE STAFF IS PRIMARILY SEEKING INSIGHTS REGARDING THE CONCEPTS IN THIS PRELIMINARY LANGUAGE AND SECONDARILY SEEKING INSIGHTS RELATED TO DETAILS SUCH AS NUMERICAL VALUES FOR VARIOUS CRITERIA.**

**STAFF DISCUSSION OF PART 73 PHYSICAL SECURITY – PRELIMINARY RULE LANGUAGE (June 2021)**

| Preliminary Language | Discussion |
|---|---|
| **PHYSICAL SECURITY FOR ADVANCED NUCLEAR REACTORS** | |
| **§ 73.100 - Technology neutral requirements for physical protection of licensed activities at advanced nuclear plants against radiological sabotage.** | The proposed new section of 10 CFR 73.100 in Part 73 provides a regulatory framework based on performance requirements that minimize or eliminate prescriptive requirements (compared to 10 CFR 73.55) to permit the applicant/licensee the maximum flexibility to determine how it will design and implement the physical protection necessary to protect against the design basis threat (DBT) and security of the plant for activities involving nuclear material. |
| (a) *Introduction*. (1) An advanced nuclear plant licensee under 10 CFR part 53 who does not meet the criterion in 10 CFR 53.830(a)(2)(i) must implement the requirements of this section through its Commission-approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Cyber Security Plan, referred to collectively hereafter as ‘‘security plans.”<br><br>(2) The security plans must identify, describe, and account for site-specific conditions that affect the licensee’s capability to satisfy the requirements of this section. | The current physical security requirements use a combination of performance criteria (e.g., the physical protection program must protect against the DBT for radiological sabotage as stated in 10 CFR 73.1) and numerous prescriptive requirements developed to achieve the performance objective. In a performance-based approach to physical security, performance criteria and objectives are the primary basis for regulatory decision making, giving the licensee the flexibility to determine how to meet the established |

| | |
|---|---|
| | performance criteria for an effective physical protection program. |
| (b) *General performance objective and requirements.* (1) The licensee must establish and maintain a physical protection program and a security organization, which will have as their objective to provide reasonable assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The design and implementation of the physical protection program must achieve and maintain at all time the capabilities for meeting the following performance requirements: | § 73.100(b) – This paragraph outlines the general performance objective and design requirements of the licensee physical protection program. Licensees are required to provide protection against the design basis threat of radiological sabotage. To accomplish this, the physical protection program is designed to protect against any deliberate act against the plant or against a component of such a plant, including spent fuel sabotage, which could directly or indirectly endanger the public health and safety by exposure to radiation. |
| (i) *Intrusion detection systems.* Physical security structures, systems, and components relied on for interior and exterior intrusion detection functions must be designed to detect attempted and actual unauthorized access. The design must provide diverse methods for achieving the intended intrusion detection functions, sufficient to ensure the reliability and availability of systems and components. | The design requirements of this section also require licensees to conduct a site specific analysis that accounts for site conditions and utilizes the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures. The physical protection program is supported by the access authorization, cyber security, and insider mitigation programs to meet the general performance objective of this section. The effectiveness of the physical protection program is measured through implementation of the performance evaluation program. |
| (ii) *Intrusion assessment systems.* Physical security structures, systems, and components relied on for intrusion assessment functions must be designed to provide rapid remote assessment for determining cause and initiating appropriate security responses. The design must provide diverse methods for achieving the intended intrusion assessment functions, sufficient to ensure the reliability and availability of systems and components. | |
| (iii) *Security communication systems.* Structures, systems, and components relied on for security communications must be designed to provide continuity and integrity of communications. Communication systems must account for design basis threats that can interrupt or interfere with continuity or integrity of communications. The design must provide diverse and redundant methods for achieving the intended communication functions. | § 73.100(b)(i) – b(vi) – The general performance objective and requirements are informed by § 73.55(b) and the Security Design Considerations that were developed in March 2017 - Non-LWR Physical and Cyber Security Design Considerations (FRN - ML17060A456). These considerations, if adequately implemented through a detailed design of the physical protection program, along with the |
| (iv) *Security delay systems.* Structures, systems, and components relied on for delay functions must be designed to provide for timely | |

| | |
|---|---|
| security responses to adversary attacks with adequate defense-in-depth.<br><br>(v) *Security response.* Engineered physical security structures, systems, and components performing neutralization functions and engineered fighting positions relied on to protect security personnel performing neutralization functions must be designed to provide overlapping fields of fire. The design configuration must provide layers of security response, with each layer assuring that a single failure does not result in the loss of capability to neutralize the design basis threat adversary.<br><br>(vi) *Control measures protecting against land and waterborne vehicle bomb assaults.* Physical security structures, systems, and components, in conjunction with site-specific natural features, that are relied on to protect against a design basis threat land vehicle and waterborne vehicle bomb assault must be designed to protect of the reactor building and structures containing safety or security related structures, systems, and components from explosive effects that are based on the maximum design basis threat quantity of explosives. The vehicle control measures (passive and active barrier systems) to deny land or waterborne vehicle bomb assaults must be located at a bounding minimum safe stand-off distance to adequately protect all structures, systems, and components required for safety and security.<br><br>(vii) *Access control portals:* Access control portals must be designed to detect and deny unauthorized access to persons and pass-through of contraband materials (e.g., weapons, incendiaries, explosives). The design must provide diverse and redundant methods for achieving the intended intrusion access control functions.<br><br>(2) To satisfy the general performance objective and requirements of paragraph (b)(1) of this section, the physical protection program must protect against the design basis threat of radiological sabotage as | adequate implementation of administrative controls and security programs, provide reasonable assurance that a licensee can protect a nuclear power reactor against the DBT of radiological sabotage. Consistent with the Commission's "Policy Statement on the Regulation of Advanced Reactors," these considerations should be considered early in the design process.<br><br>The performance objective of protecting against the DBT of radiological sabotage is achieved by the design and implementation of the physical protection program, maintained at all times, with the following performance requirements:<br><br>• *Intrusion detection systems*<br>• *Intrusion assessment systems*<br>• *Security communication systems.*<br>• *Security delay systems*<br>• *Security response*<br>• *Control measures protecting against land and waterborne vehicle bomb assaults*<br>• *Access control portals*<br><br>The proposed performance requirements permit the designer/applicant/licensee to determine how to design the physical protection program to protect the plant against the DBT of radiological sabotage, without the constraints of prescriptive requirements such as those currently found in 10 CFR 73.55.<br><br>§ 73.100(b)(2) –This proposed section is developed from 73.55(b)(3). The proposed language removes reference to "significant core damage," which applies |

| | |
|---|---|
| stated in § 73.1 of this part. Specifically, the licensee must<br><br>(i) Ensure that the physical protection program capabilities to protect against the design basis threat of radiological sabotage are maintained at all times.<br><br>(ii) Provide defense-in-depth in achieving performance requirements through the integration of engineered systems, administrative controls, and management measures to assure effectiveness of the physical protection program to protect the plant against the design basis threat of radiological sabotage.<br><br>(3) The licensee must identify and analyze site-specific conditions that may affect the physical protection program needed to implement the requirements of this section. The licensee must account for these conditions in meeting the requirements of this section. | mainly to light-water reactor technology, and focuses on radiological sabotage in order to be technology neutral and incorporate the rationale from the limited scope Physical Security for Advanced Reactors Rulemaking that is currently ongoing.<br><br>Defense-in-depth – The designs of physical security systems should employ defense-in-depth through systems diversity, independence, and separation to achieve reasonable assurance that intended security functions meet all performance criteria. The defense-in-depth philosophy applies to measures against intentional acts. The most common defense-in-depth measures apply concepts of redundancy, diversity, independence, and safety margin to enhance systems reliability. Defense-in-depth is achieved by providing multiple layers of protection, systems, and/or barriers to avoid (or provide the capability to tolerate) failures that would prevent the accomplishment of a function. Diversity and separation provide protection against dependent failures of multiple (usually identical) means of accomplishing needed functions due to a shared cause (i.e., common cause failures). Operational requirements (i.e., security responses providing interdiction and neutralization functions) provide defense-in-depth by using layers of protection and by accounting for uncertainties (e.g., equipment malfunction, human factors, neutralized or operationally ineffective responses, etc.) to perform required interdiction and neutralization function at all plant areas. The NRC's philosophy applies to the design of a physical protection program, which integrates engineered controls and administrative controls, to provide reasonable assurance of protection against the DBT for radiological sabotage. |

| | |
|---|---|
| (4) The licensee must establish, maintain, and implement a performance evaluation program to assess the effectiveness of the licensee's implementation of the physical protection program to protect against the design basis threat of radiological sabotage. | § 73.100(b)(4) – The performance evaluation program periodically tests and evaluates the effectiveness of the physical protection program designed to protect against the DBT, including the security response performing the functions of interdiction/neutralization for implementing the licensee protective strategy. |
| (5) The licensee must establish, maintain, and implement an access authorization program in accordance with § 73.56 and must describe the program in the Physical Security Plan. | § 73.100(b)(5) – Implement an access authorization program in accordance with § 73.56. |
| (6) The licensee must establish, maintain, and implement a cyber security program in accordance with § 73.110 and must describe the program in the Cyber Security Plan. | § 73.100(b)(6) – Establish, maintain, and implement protection against a cyber attack based on the proposed cyber security program described in § 73.110. This is an alternative to of the program described in § 73.54. |
| (7) The licensee must establish, maintain, and implement an insider mitigation program and must describe the program in the Physical Security Plan.<br>(i) The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access or unescorted access authorization, and implement defense-in-depth methodologies to minimize the potential for an insider (active, passive, or both) to adversely affect, either directly or indirectly, the licensee's capability to protect against radiological sabotage.<br>(ii) The insider mitigation program must integrate elements of:<br>(A) The access authorization program described in § 73.56;<br>(B) The fitness-for-duty program described in part 26 of this chapter;<br>(C) The cyber security program described in § 73.110; and<br>(D) The physical protection programs described in this section. | § 73.100(b)(7) – Insider mitigation measures and program to protect against the DBT insider (passive, active, and violent). |

| | |
|---|---|
| (8) The licensee must use the site corrective action program to track, trend, correct, and prevent recurrence of failures and deficiencies in the implementation of the requirements of this section.<br><br>(9) Implementation of security operations and plans must be coordinated with plant operations and plans to preclude conflict during both normal and emergency conditions and ensure the adequate management of the safety and security interface.<br><br>(c) *Security organization*. The licensee must establish and maintain a security organization that is staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of this section.<br><br>(1) The licensee must establish a management system for maintaining and implementing security policies and procedures to implement the requirements of this section and the security plans.<br><br>(2) Implementing procedures must document the conduct of security operations, design and configuration controls, maintenance, training and qualification, and contingency responses.<br><br>(3) The licensee must:<br><br>(i) Establish a process for the approval of designs, policies, processes, and procedures and changes by the individual with overall responsibility for the physical protection program.<br>(ii) Ensure that revisions and changes to the physical protection program and implementing policies, processes, and procedures satisfy the requirements of this section.<br><br>(4) The licensee must retain, in accordance with § 73.70, all analyses, assessments, calculations and descriptions of the technical basis for meeting the performance requirements of § 73.100(b). Safeguards information must protect these records in accordance with the requirements of § 73.21. | § 73.100(c) – This paragraph outlines the requirements for the composition, equipping, and training of the security organization. The intent is that the security organization will focus on the effective implementation of the physical protection program. Individuals assigned to perform physical protection or contingency response duties must be trained, equipped, and qualified to perform assigned duties and responsibilities whether that individual is a member of the security organization or not. Developed from § 73.55(b)(7) Security implementing procedures and § 73.55(d) Security organization. |

| | |
|---|---|
| (5) The licensee may not permit any individual to implement any part of the physical protection program unless the individual has been trained, equipped, and qualified to perform their assigned duties and responsibilities in accordance with the Training and Qualification Plan. | |
| (d) *Search requirements*. The licensee must establish and implement searches to detect and prevent the introduction of firearms, explosives, incendiary devices, or other items and material which could be used to commit radiological sabotage. The program must accomplish this through search of individuals, vehicles, and materials consistent with the performance requirements of paragraph (b)of this section. | § 73.100(d) – This paragraph establishes a performance requirement for searches of personnel, vehicles, and materials for the protection against radiological sabotage. The rule text eliminates the categorization of it as a "program." The broad categories of material (explosives, firearms, incendiary devices, etc.) that will be prohibited are not prescribed but will be stated in the licensee security plans with detailed descriptions being identified in implementation procedures. |
| (e) *Security reviews*. The licensee must establish and implement security reviews to assess the effectiveness of the implementation of the physical protection program and the requirements in this section. Security reviews must be performed by individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program<br><br>(1) The licensee must review each element of the physical protection program at a frequency commensurate with the importance or significance to safety of plant operations, to ensure timely identification and documentation of vulnerabilities, improvements, and corrective actions. The objective of these reviews must be maintaining effective implementation of the engineered and administrative controls required to achieve the physical protection program functions and the management system required to implement programs and requirements in this section.<br><br>(2) The licensee must establish, maintain, and perform a | § 73.100(e) – This paragraph ensures effective implementation of the physical protection program and through periodic reviews of the program. This proposed rule text was developed from 73.55(m) to review each element of the physical protection program by individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program. |

| | |
|---|---|
| self-assessment to ensure the effective implementation of the physical protection program functions of detection, assessment, communication, delay, and interdiction and neutralization to protect against the design basis threat of radiological sabotage. The licensee must perform design verification and assessments of the capabilities of active and passive engineering systems relied on to protect against the design basis threat.<br><br>(f) *Performance evaluation.* Licensee performance evaluation must:<br><br>(1) establish methods appropriate and necessary to assess, test, and challenge the integration of the physical protection program's functions to protect against the design basis threat, measures protecting against cyber attack, and engineered systems designed to protect against the design basis threat standalone ground vehicle bomb attack.<br><br>(2) The licensee must establish the appropriate and necessary frequencies for performance evaluations, verifications, and assessments based on the importance, security significance, reliability, and availability of physical protection program functions and implementation of programs and requirements in this section.<br><br>(3) The licensee must document processes and procedures and maintain records, including results, findings, and corrective actions, for implementing the performance evaluations, verifications, and assessments. | |
| (g) *Maintenance, testing, and calibration and corrective actions*. (1) The licensee must ensure that security systems and equipment, including supporting systems, are inspected, tested, and/or calibrated for operability and performance at intervals necessary and sufficient to meet the requirements in this section.<br><br>(2) The licensee must implement corrective actions necessary and sufficient to ensure resolution of identified vulnerabilities and deficiencies to meet the requirements in this section. | § 73.100(g) – This paragraph establishes performance requirements for maintaining security structures, systems, or components (SSC) relied on to perform security functions to protect against the DBT and implementing security programs. It includes corrective actions to be taken by a licensee in response to a failure or degradation of security equipment to perform its intended functions and implementation of security programs. The draft rule requires that the licensee will maintain the SSCs |

| | |
|---|---|
| (3) The licensee must establish and implement timely compensatory measures for degraded or inoperable security systems, equipment, and components to meet the requirements of this section. Compensatory measures must provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable, systems, equipment, or components.<br><br>(4) The licensee must document processes and procedures and maintain records for implementing the corrective actions, compensatory measures, and maintenance, inspection, testing, and calibration of security structures, systems, and equipment. | described in its design and licensing basis to assure that they are reliable and available. |
| (h) *Suspension of security measures*. (1) The licensee may suspend implementation of affected requirements of this section in accordance with §§ 50.54(x) and 50.54(y) of this chapter under the following conditions:<br><br>(i) In an emergency, when action is immediately needed to protect the public health and safety; and<br><br>(ii) During severe weather, when the suspension of affected security measures is immediately needed to protect the personal health and safety of personnel.<br><br>(2) Suspended security measures must be reinstated as soon as conditions permit.<br><br>(3) The suspension of security measures must be reported and documented in accordance with the provisions of § 73.71. | § 73.100(h) – This paragraph establishes requirements for the suspension of security measures in response to emergency and extraordinary conditions. The requirements of this paragraph are intended to provide flexibility to a licensee for taking reasonable actions that depart from an approved security plan in an emergency when such actions are immediately needed to protect the public health and safety and no action consistent with license conditions and technical specifications that can provide adequate or equivalent protection is immediately apparent in accordance with § 50.54(x) and (y) or similar applicable regulations as identified in Part 53. |
| (i) *Records*. (1) The licensee must maintain all records required to be kept by Commission regulations, orders, or license conditions, until the Commission terminates the license for which the records were developed, and must maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.<br><br>(2) If a contracted security force is used to implement the onsite physical protection program, the licensee's written agreement with | |

| | |
|---|---|
| the contractor must be retained by the licensee as a record for the duration of the contract.<br><br>(3) All records must be available for inspection, for a period of 3 years. | |