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. WHILE THE NRC WILL CONSIDER ALL COMMENTS RECEIVED IN FURTHER DEVELOPING THE PRELIMINARY LANGUAGE, IT WILL NOT PROVIDE WRITTEN RESPONSES TO THOSE COMMENTS. ONCE THE PROPOSED RULE IS ISSUED IN THE *FEDERAL REGISTER*, THE PUBLIC WILL HAVE AN ADDITIONAL OPPORTUNITY TO PROVIDE COMMENTS AND THE AGENCY WILL RESPOND IN WRITING TO ALL PUBLIC COMMENTS ON THE PROPOSED RULE WHEN ISSUING A FINAL RULE.

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

Preliminary Language	Discussion
PHYSICAL SECURITY FOR ADVANCED NUCLEAR REACTORS	
§ 73.100 - Technology ~~neutral~~inclusive requirements for physical protection of licensed activities at ~~advanced~~commercial nuclear plants against radiological sabotage.	The proposed section of 10 CFR 73.100 in Part 73 provides a regulatory framework based on performance requirements that minimize prescriptive requirements (compared to 10 CFR 73.55) to permit the applicant/licensee 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~~A commercial nuclear plant licensee under 10 CFR part 53 ~~who does not meet the criterion in 10 CFR 53.830(a)(2)(i) must~~ that elects to implement the requirements of this section must do so through its Commission-approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Cyber Security Plan, referred to collectively	Incorporated stakeholder comment to remove specific applicability to only licensees that do not meet the criteria in § 53.830(a)(2)(i). If a licensee doesn't meet the criterion, they must choose between this section and § 73.55; if they do meet the criterion, they may also choose to voluntarily implement these

hereafter as ‘‘security plans.” ,” before initial fuel load into the reactor. (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. (b) *General performance objective and requirements.* (1) The licensee must establish, implement, 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. (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 stated in § 73.1 of this part. Specifically, the licensee must (i) Ensure that the physical protection program capabilities to protect against the design basis threat of radiological sabotage are maintained at all times. (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. (3) The physical protection program must be designed and implementedation of the physical protection program must to achieve and maintain the reliability and availability of security structures, systems, and components. The physical protection program must achieve and maintain at all time the capabilities for meeting the following performance requirements: (i) *Intrusion detection systems.* Physical security structures, systems, and components relied on for interior and exterior intrusion detection functions. The licensee must be designed to	requirements. § 73.100(b) – added “implement” for consistency with other edits to this section. The preliminary rule language in § 73.100(b)(1)(i) – (vi) in the first iteration was moved to § 73.100(b)(3) to address stakeholder comments and assist with flow of requirements. This change is not shown in the redline strike out to aid in readability of text and only highlight edits to text and not format/location changes. § 73.100(b)(3) – These requirements were streamlined to remove repetitive rule text and to rewrite the requirements based on stakeholder feedback. The text was changed from what the structures, systems, and components must be designed to accomplish to what the licensee must be capable of performing.

~~detect~~capable of detecting attempted and actual unauthorized access to interior and exterior areas containing equipment needed to implement safety and security functions. ~~The design must provide diverse methods for achieving the intended intrusion detection functions, sufficient to ensure the reliability and availability of systems and components~~ (ii) ~~*Intrusion assessment systems.* Physical security structures, systems, and components relied on for intrusion assessment functions.~~ The licensee must be ~~designed to provide~~ capable of rapid ~~remote~~ assessment for determining cause ~~and initiating appropriate security responses~~of a detected intrusion. ~~. 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~~. The licensee must be capable of continuous 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.~~ ~~(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.~~ *(iv) Security response*. The licensee must be capable of timely security response to interdict and neutralize adversary attacks up to and including the design basis threat of radiological sabotage. ~~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 physical protection program must be designed to ~~configuration must~~ provide layers of security response, with each layer assuring that a	Security delay systems – The separate security delay systems language in the paragraph that was previously § 73.100(b)(3)(iv) was combined in this iteration with security response in the now renumbered § 73.100(b)(3)(iv). Delay enables timely response by impeding the adversary.

single failure does not result in the loss of capability to neutralize the design basis threat adversary. 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. (vi) *Control measures pProtecting against land and waterborne vehicle bomb assaults.* Physical security structures, systems, and components, in conjunction with site-specific natural features,The licensee must be capable of protecting the plant against the design basis threat vehicle bomb assault. The methods 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. (vii) *Access control portals.: Access control portals* The licensee must be designed to capable of detecting and denying unauthorized access to persons and pass-through of contraband materials (e.g., weapons, incendiaries, explosives) to protected areas. The design must provide diverse and redundant methods for achieving the intended intrusion access control functions. (4) The licensee must meet the requirements related to target sets in § 73.55(f). (53) The licensee must identify and analyze site-specific conditions, including target sets, 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. (64) The licensee must establish, implement, and maintain, and implement, a performance evaluation program to assess the	(v) Protecting against land and waterborne vehicle bomb assaults - Removed the reference to 'minimum safe stand off distance." This language is better suited for guidance. § 73.100(b)(4) requires the licensee to identify target sets in accordance with §§ 73.55(f)(1) through (4). Based on stakeholder interactions the staff reconsidered this requirement. In this iteration, the licensee must identify the minimum combination of equipment and what needs to be protected in order to design the physical security program to meet the performance objective of § 73.100(b).

effectiveness of the licensee's implementation of the physical protection program to protect against the design basis threat of radiological sabotage. (7~~5~~) The licensee must establish, implement, and maintain ~~, and implement~~ an access authorization program in accordance with § 73.56 and must describe the program in the Physical Security Plan. (8~~6~~) The licensee must establish, implement, and maintain~~, and implement~~ a cyber security program in accordance with §§ 73.54 or 73.110 and must describe the program in the Cyber Security Plan. (9~~7~~) The licensee must establish, implement, and maintain~~, and implement~~ an insider mitigation program and must describe the program in the Physical Security Plan. (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 to a protected or vital area, 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. (ii) The insider mitigation program must integrate elements of: (A) The access authorization program described in § 73.56; (B) The fitness-for-duty program described in part 26 of this chapter; (C) The cyber security program described in §§ 73.54 or 73.110; and (D) The physical protection program~~s~~ described in this section. (10~~8~~) The licensee must have the capability ~~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. (11~~9~~) Implementation of security operations and plans must be coordinated with plant operations and plans to preclude conflict	§ 73.100(b)(9) - This language was edited to match § 73.55 and include specific access locations in which the insider mitigation program must apply. This change is based on the overall comment related to protected and vital areas and remaining consistent with § 73.55 terminology and other part 73 regulations. The staff is further reviewing if more prescriptive regulations, related to protected and vital area identification are necessary. (Compare to §§ 73.55(e)(8) and (9)) § 73.100(b)(10) – edited based on stakeholder feedback.

during both normal and emergency conditions and ensure the adequate management of the safety and security interface.

(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.

(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.

(2) Implementing procedures must document the conduct of security operations, security design and configuration controls, maintenance, training and qualification, and contingency responses.

(3) The licensee must:

(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.

(ii) Ensure that revisions and changes to the physical protection program and implementing policies, processes, and procedures satisfy the requirements of this section.

(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 The licensee must protect these records in accordance with the requirements of for protecting safeguards information in §§ 73.21 and 73.22.

(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 of individuals, vehicles, and materials to detect and prevent the introduction into the protected area 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.~~ (e) *Training and qualification program.* The licensee must establish and maintain a training and qualification program that ensures personnel who are responsible for the physical protection of the facility against radiological sabotage are able to effectively perform their assigned security-related job duties for implementing the requirements of this section and must describe the program in the Training and Qualification Plan. (f~~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. (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. (2) The licensee must establish~~, maintain,~~ and perform ~~a~~ self-assessments 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	§ 73.100(e) – This high-level requirement allows more flexibility in how the licensee chooses to protect the site. One method for accomplishing this requirement would be to provide a training and qualification program equivalent to Part 73, Appendix B. § 73.100(f) – This paragraph ensures effective implementation of the physical protection programs and through periodic reviews of the program. This proposed rule text was developed from § 73.55(m) to review each element (§ 73.100(f)(1)) 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. § 73.100(f)(2) addresses the intended overall performance function (multiple elements) to ensure that the capability to detect, assess, interdict, and neutralize the DBT of radiological sabotage is maintained.

capabilities of active and passive engineering systems relied on to protect against the design basis threat.

(3) Reviews of the security program must include, but are not limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.

(4) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report and must be maintained in an auditable form and available for inspection.

(gf) *Performance evaluation*. Licensee performance evaluation must:

(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, including measures protecting against cyber attack, and engineered systems designed to protect against the design basis threat standalone ground vehicle bomb attack.

(12) 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.

(23) The licensee must document processes and procedures and maintain records, including results, findings, and corrective actions, for implementing the performance evaluations, verifications, and assessments. The licensee must maintain records, including results, findings, and corrective actions identified during the performance evaluations.

(hg) *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. (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. (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 prior to the ~~by the~~ degradation~~ed~~ or inoperability~~le,~~ of the security systems, equipment, or components. (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. (~~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~~§§ 53.755(j) and (k) under the following conditions: (A~~i~~) In an emergency, when action is immediately needed to protect the public health and safety; and (B~~ii~~) During severe weather, when the suspension of affected security measures is immediately needed to protect the personal health and safety of personnel. (2) Suspended security measures must be reinstated as soon as conditions permit. (3) The suspension of security measures must be reported and documented in accordance with the provisions of § 73.71. (~~i~~) *Records*. (1) The Commission may inspect, copy, retain, and remove all reports, records, and documents required to be kept by	

Commission regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor. (2) 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. (~~2~~3) 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. (~~3~~4) ~~All records~~Review and audit reports must be available for inspection, for a period of 3 years.	