From:	YOUNG, David
To:	Valliere, Nanette
Cc:	Atack, Sabrina; Gavrilas, Mirela; Beall, Bob; Andrukat, Dennis; Lee, Pete
Subject:	[External_Sender] Comments on Part 53 Rule Language
Date:	Monday, June 14, 2021 5:43:59 PM
Attachments:	Mark-up of 10 CFR 73-100 with Eligibility Criteria.pdf

Nan,

Good afternoon.

We appreciated the opportunity for NEI and our members to provide comments on the portions of the proposed Part 53 rule language presented during last Thursday's public meeting. To ensure a clear understanding of our comments, we have summarized them below.

1. The proposed 10 CFR 73.100 (in the Part 53 rulemaking) appears to require an onsite armed response force to interdict and neutralize an adversary. The requirements in the proposed 10 CFR 73.55 (in the Alternative Physical Security Requirements rulemaking) permit a licensee to rely on local law enforcement to interdict and neutralize. We're unclear why the approach (e.g., eligibility criteria) in 10 CFR 73.55 is not being carried over to 10 CFR 73.100, and believe it should be. Attached is a marked-up version of the proposed 10 CFR 73.100 showing an example of how this comment might be addressed by incorporating the eligibility criteria in the proposed 10 CFR 73.55.
2. Despite dialog in this public meeting and previous exchanges, we still do not understand the staff's expectations for performing an analysis of a "hypothetical unmitigated event," as the term is used in the proposed 10 CFR 73.55 and 10 CFR 73.100. In addition, some heard staff answers last week that led them to believe that the requirements for the analysis could be different depending upon which regulation the applicant is attempting to meet. We continue to believe that "hypothetical" should be removed (absent a clearly articulated basis for its retention) and the analysis performed with credit for all features described in the facility licensing basis but no operator/manual actions (i.e., unmitigated).
3. In general, our feeling is that new requirements should 1) clearly identify facility criteria that permit reliance on local law enforcement to interdict and neutralize (so designers know) and 2) allow maximum flexibility in the design of physical protection elements. We also suggest the staff seek stakeholder input on the "hypothetical unmitigated event" criterion – as the staff envisions it, is this a criterion that anyone can meet/use?
4. Other comments we made during the meeting include:
    a. The rule requires compliance with Part 26 (FFD) and 10 CFR 73.56 (Access Authorization). These regulations include requirements related to a Protected Area (PA) and Vital Areas (VAs). The proposed 10 CFR 73.100 does not address establishment of PAs or VAs. How will this apparent inconsistency be addressed? A detailed review may be needed to identify other changes to ensure consistency across regulations.
    b. Proposed 10 CFR 73.100(b)(vii) requires access control portals – it does not

indicate the area or boundary to which the access controls apply.

c. Proposed 10 CFR 73.100(b)(8) requires use of a corrective action program – to provide flexibility for future licensees, it may be desirable to instead provide performance-based criteria for this requirement. See attached mark-up for an example.
d. Proposed 10 CFR 73.100(d) requires searches - it does not indicate the area or boundary to which search requirements apply.
e. Proposed 10 CFR 73.100(e) requires "Security reviews" – Does the NRC have information concerning the potential value of this requirement (i.e., what's the OE from the current fleet after doing these reviews for decades)? Can it be time limited? For example, can it be terminated after a certain number of reviews are completed?

Feel free to contact me with any questions.

David Young | *Technical Advisor*
Nuclear Security and Incident Preparedness
Nuclear Energy Institute
(202) 739-8127

§ 73.100 - Technology neutral requirements for physical protection of licensed activities at advanced nuclear plants against radiological sabotage.

(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."

(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. ~~The design and implementation of the~~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 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,~~be 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 of a detected intrusion and initiating appropriate security responses. The design must ~~provide diverse methods for achieving the intended intrusion assessment functions,~~be sufficient to ensure the reliability and availability of systems and components.

(iii) Security ~~communication systems. Structures, systems, and components relied on for security~~ communications. The licensee must be ~~designed to provide continuity and integrity~~capable of security 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~~be sufficient to ensure the reliability and availability of systems and components.

~~(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-indepth.~~

~~(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.~~ (iv) Security response. A licensee of a small modular reactor, as defined in 10 CFR 171.5, or non-light water reactor that satisfies one or more of the eligibility criteria in § 73.100(b)(iv)(A), (B), or (C) may rely on local law

enforcement to perform security response neutralization functions. The licensee must identify each eligibility criterion satisfied and perform and submit to the NRC an analysis that demonstrates how the identified criterion is met. All other licensees must be capable of performing neutralization functions.

(A) The radiological consequences from an unmitigated event involving the loss of engineered systems for decay heat removal and possible breaches in physical structures surrounding the reactor, spent fuel, and other inventories of radioactive materials result in offsite doses below the reference values defined in §§ 50.34(a)(1)(ii)(D) and 52.79(a)(1)(vi) of this chapter; or

(B) The plant features necessary to mitigate an event and maintain offsite doses below the reference values in §§ 50.34(a)(1)(ii)(D) and 52.79(a)(1)(vi) of this chapter cannot reasonably be compromised by an adversary as defined by the design basis threat for radiological sabotage; or

(C) Plant features include inherent reactor characteristics combined with engineered safety and security features that allow for facility recovery and mitigation strategy implementation if a target set is compromised, destroyed, or rendered nonfunctional, such that offsite radiological consequences are maintained below the reference values defined in §§ 50.34(a)(1)(ii)(D) and 52.79(a)(1)(vi) of this chapter.

~~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.~~

~~(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.~~

~~(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.~~

(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 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.

~~4) The licensee must establish, maintain, and implement~~(4) 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.

(5) 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.

(6) 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.

(7) A licensee required to perform neutralization functions must establish, implement, and maintain a site protective strategy that incorporates 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.

(8) The licensee must establish, implement, and maintain 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.

(~~5~~9) The licensee must establish, ~~maintain, and~~ implement, and maintain an access authorization program in accordance with § 73.56 and must describe the program in the Physical Security Plan.

(~~6~~10) The licensee must establish, ~~maintain, and~~ implement, and maintain a cyber security program in accordance with § 73.110 and must describe the program in the Cyber Security Plan.

(~~7~~11) The licensee must establish, ~~maintain, and~~ implement, and maintain 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, 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 § 73.110; and

(D) The physical protection programs described in this section.

~~8~~(12) The licensee must ~~use~~have the ~~site corrective action program~~capability to track, trend, correct, and prevent recurrence of failures and deficiencies in the implementation of the requirements of this section.

(~~9~~13) 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.

(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, 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 must protect these records in accordance with the requirements of § 73.21.

(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.

~~(b)of this section.~~

(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-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.

(f) Performance evaluation. ~~Licensee~~The 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, measures protecting against cyber attack, and engineered systems designed to protect against the design basis threat standalone ground vehicle bomb attack.

(~~2~~1) 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.

(~~3~~2) 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.

(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 by the degraded or inoperable, 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 under the following conditions:

(i) In an emergency, when action is immediately needed to protect the public health and safety; and

(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 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) 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) All records must be available for inspection, for a period of 3 years.