INL/MIS-26-91941

ADVANCED REACTOR SAFEGUARDS & SECURITY

Performance-Based Physical Security Framework – FY26

ARSS Spring / Summer Program Review

PRESENTED BY

Christopher Chwasz

April 29, 2026

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories | U.S. DEPARTMENT OF ENERGY

Part 53 Rulemaking

- Posted in the Federal Register 3/30/2026
- Entirely new technology-neutral licensing framework from Part 50
- Requires security by design - **§** 53.440(f)
- Provides **performance-based security alternatives**

10 CFR 53.860:

(a) *Physical protection program.* Each holder of an OL or COL under this part must develop, implement, and maintain a physical protection program under the following requirements:

(1) The licensee must implement security requirements for the protection of special nuclear material based on the type, enrichment, and quantity in accordance with 10 CFR part 73, as applicable, and implement security requirements for the protection of Category 1 and Category 2 quantities of radioactive material in accordance with 10 CFR part 37, as applicable; and

(2) The licensee must demonstrate compliance with the provisions set forth in either § 73.55 or **§ 73.100** of this chapter.

(b) *Fitness-for-duty.* Each holder of an OL or COL under this part must develop, implement, and maintain a fitness-for-duty program under 10 CFR part 26. **(Part 26 Subpart M—Fitness-for-Duty Programs for Facilities Licensed Under 10 CFR Part 53)**

(c) *Access authorization.* Each holder of an OL or COL under this part must develop, implement, and maintain an access authorization program under § 73.56 or **§ 73.120** of this chapter, as applicable.

(d) *Cybersecurity.* Each holder of an OL or COL under this part must develop, implement, and maintain a cybersecurity program under § 73.54 or **§ 73.110** of this chapter.

Part 53 Rulemaking – Guidance

RG #	Title	Rev	Publish Date	Draft Guide #	ML#
5.81	Target Set Identification and Development for Nuclear Power Reactors (OUO-SRI)	2	3/2026	DG-5071	ML24229A186 See NRC
~~5.94~~	~~Fitness-For-Duty Programs for Commercial Nuclear Plants and Manufacturing Facilities Licensed Under 10 CFR Part 53~~	~~0~~	~~3/2026~~	~~DG-5073~~	rolled into Rule language and RG 5.99
5.95	Access Authorization Program for Commercial Nuclear Plants	0	3/2026	DG-5074	ML25232A007
5.96	Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53	0	3/2026	DG-5075	ML25232A008
5.97	Guidance for Technology Inclusive Requirements for Physical Protection of Licensed Activities at Commercial Nuclear Plants	0	3/2026	DG-5076	ML25232A009
5.99	Fatigue Management for Nuclear Power Plant Personnel at Commercial Nuclear Plants Licensed Under 10 CFR Part 53	0	3/2026	DG-5078	ML25232A010

Part 53 Rulemaking – §73.100

(a) *Introduction.*

(1) Each licensee that is licensed to operate a commercial nuclear plant under part 53 of this chapter and elects to implement the requirements of this section must identify achievable target sets in accordance with paragraph (b)(5) of this section and develop, implement, and maintain a physical protection program under the following requirements:

(i) Each licensee that demonstrates **no achievable target sets exist** in accordance with paragraph (b)(5) of this section, and **does not credit any active measures** (*e.g.,* operator action, mitigative action, detection, assessment, armed response) in making that demonstration, is **exempt from the remaining requirements of this section.**

(ii) Each licensee that demonstrates **no achievable target sets exist** in accordance with paragraph (b)(5) of this section, and **credits active measures** in making that demonstration, must implement the requirements of this section through its physical security plan, training and qualification plan, safeguards contingency plan, and cybersecurity plan, referred to collectively hereafter as "security plans," before initial fuel load into the reactor (or, for a fueled manufactured reactor, before initiating the removal of the features to prevent criticality required under § 53.620(d)(1) of this chapter); for such licensees, the **requirements of paragraphs (b)(2) through (4) of this section will be deemed satisfied if the physical protection program is designed to ensure that the credited active measures will be implemented** in response to threats up to and including the design-basis threat of radiological sabotage.

(iii) **Each licensee that demonstrates achievable target sets exist**, in accordance with paragraph (b)(5) of this section, must implement the requirements of this section through its physical security plan, training and qualification plan, safeguards contingency plan, and cybersecurity plan, referred to collectively hereafter as "security plans," before initial fuel load into the reactor (or, for a fueled manufactured reactor, before initiating the removal of the features to prevent criticality required under § 53.620(d)(1) of this chapter).

(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.

Part 53 Rulemaking – §73.100

(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 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. 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; and

(ii) Provide defense in depth in achieving performance requirements through the integration of engineered systems, administrative controls, and management measures.

(3) The physical protection program must be designed to prevent the release of radionuclides from any source from exceeding the dose reference values defined in § 53.210 of this chapter.

(4) The physical protection program must be designed and implemented to achieve and maintain the **reliability and availability** of structures, systems, and components (SSCs) required for demonstrating compliance with the following performance requirements **at all times**:

(i) *Intrusion detection.*

(ii) *Intrusion assessment.*

(iii) *Security communication.*

(iv) *Security response. (to include offsite response)*

(v) *Protecting against land and waterborne vehicle bomb assaults.*

(vi) *Access control portals.*

(5) The licensee must identify and document complete and accurate target sets…

Part 53 Rulemaking – §73.100

(b) *General performance objective and requirements.* (cont.)

(6) The licensee must identify and analyze site-specific conditions…

(7) The licensee must establish, implement, and maintain a performance evaluation program…

(8) The licensee must establish, implement, and maintain an access authorization program…

(9) The licensee must establish, implement, and maintain a cybersecurity program…

(10) The licensee must establish, implement, and maintain an insider mitigation program…

(11) The licensee must have the capability to track, trend, correct, and prevent recurrence of failures and deficiencies in the implementation of the requirements of this section.

(12) Implementation of security plans and associated procedures must be coordinated with other onsite plans and procedures to preclude conflict during both normal and emergency conditions and ensure the adequate management of the safety and security interface.

(13)(i) The licensee must ensure that the firearms background check requirements of § 73.17 of this part are met

RG 5.97 - Guidance For Technology-Inclusive Requirements For Physical Protection Of Licensed Activities At Commercial Nuclear Plants

Section B. Discussion

1. Security by Design (10 CFR 53.440(f))
2. Security Operations Program
3. 10 CFR 73.100 – Performance-Based Framework
   Achievability of target sets
4. General Performance Objective and Requirements

RG 5.97- B. 4. General Performance Objective and Requirements

4.1.1 Intrusion Detection—10 CFR 73.100(b)(4)(i)

Consistent with 10 CFR 73.100(b)(4)(i), the design of physical security SSCs relied on for interior and exterior intrusion detection functions must provide assurance of detecting unauthorized access into vital and protected areas. The design should be **redundant**, independent, and diverse to ensure the reliability and availability of systems and components to achieve the intended intrusion detection functions.

4.1.2 Intrusion Assessment—… **redundant**, independent, and diverse…

4.1.3 Security Communication—…**redundant**, independent, and diverse…

4.1.4 Security Response/Neutralization—…**redundant**, independent, and diverse…

4.1.6 Access Control Portals—…**redundant**, independent, and diverse…

FY25-26 Project: Performance-based Framework

- Designed to:
  - Meet §73.100
  - Be consistent with RG 5.97 section B.4
  - Be used for 73.55:
    - 73.55(r) alternative measures
    - Via exemption process
  - Credit:
    - Offsite response (private or local law enforcement)
    - Adversary interference preclusion time / reasonable assurance of protection time
    - Allowed operator recovery and mitigating actions
    - Advanced security technologies
    - Security-by-design methods and alternative protective strategies consistent with advanced and small modular reactors

FY25-26 Project: Performance-based Framework: Process

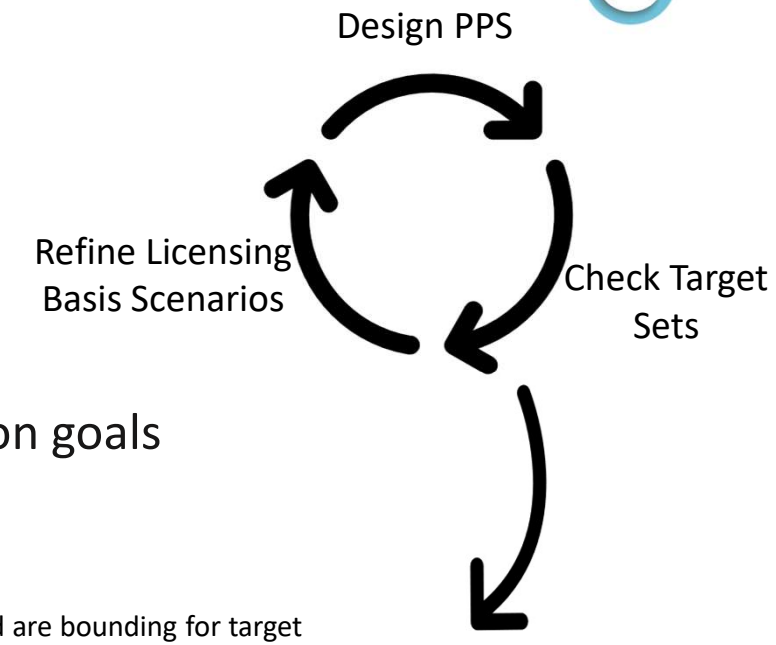
1. Target Set Analysis - Initial screen / categorization (RG 5.81 and 5.97)
2. Build DBT Licensing Basis Scenarios for remaining target sets
3. Design Physical Protection System (PPS)
    1. Iterate on PPS design
    2. Re-screen / categorize target sets (RG 5.81 and 5.97)
    3. Refine Licensing Basis Scenarios
4. Security Margin
5. Validate
6. Document in design and operational documents

FY25-26 Project: Performance-based Framework: Process

1. Target Set Analysis
    1. Unachievable
        1. Unachievable by adversary action / no active measures (**screened**) (73.100(a)(1)(i))
        2. Unachievable (Preventable) with site actions before / during event (timeline noted, **can use delay**) (73.100(a)(1)(ii))
        3. Unachievable (Mitigatable / reversible) by site actions or offsite response actions after event (timeline noted, **may use delay or denial**) (73.100(a)(1)(ii))(RG 5.97 App. C)
    2. Achievable
        1. Un-mitigatable / irreversible (**must use denial**) (RG 5.81)
2. Build Initial Licensing Basis scenarios for remaining target sets
    1. Preventable target sets (delay)
    2. Mitigatable target sets (delay or denial)
    3. Un-mitigatable target sets (denial)

FY25-26 Project: Performance-based Framework: Process

3. Design and Iterate PPS
    1. Target sets
        1. Preventable target sets (delay)
        2. Mitigatable target sets (delay or denial)
        3. Un-mitigatable target sets (denial)
    2. Determine AIPT
    3. Redesign PPS to meet Target Set categorization goals
    4. Refine Licensing Basis Scenarios

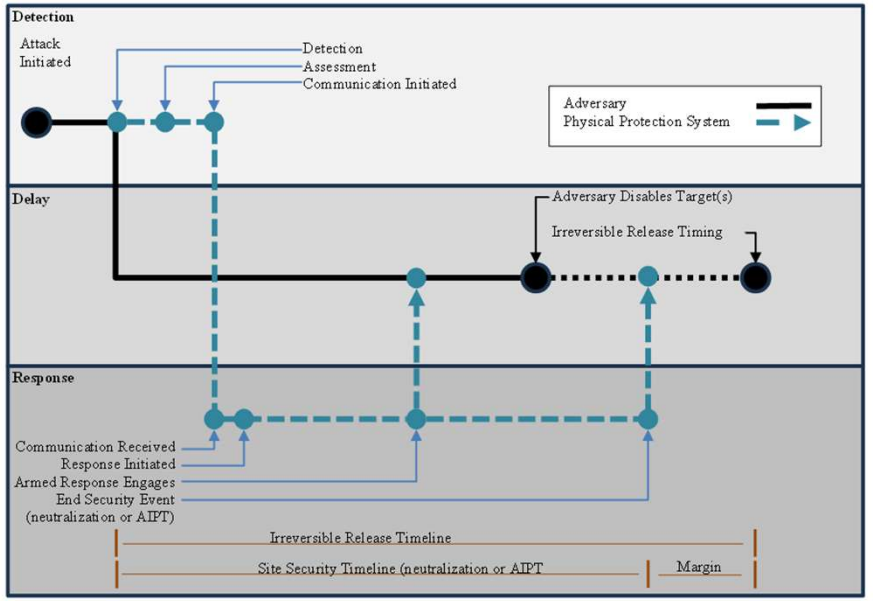


Exit when:

- Licensing Basis Scenarios best represent DBT and are bounding for target
- PPS meets delay timeline goals or neutralization as needed
- All target sets can be categorized as best they can (unachievable, unachievable with pre- or post-event actions, achievable)

FY25-26 Project: Performance-based Framework: Process

4. Security Margin
    1. Compensatory measures
    2. Defense-in-depth (DID) analysis
        1. Redundancy
        2. Sensitivity analysis
        3. Risk-informed and performance-based DID method
            1. With element “deletion” timeline no more than 10% of than the acceptable value
    3. Timeline margin



FY25-26 Project: Performance-based Framework: Process

5. Validate
    1. Component / Limited-Scope Performance Testing / TTXs / FOFs
    2. Security Program Reviews and Audits
6. Document
    1. Document Performance Parameters
        1. Irreversible Release Timing
        2. Site Security Timeline
        3. Detection Probability and Confidence
        4. System Effectiveness
    2. Technical Reports for Initial Licensing
        1. Licensing Basis Events
        2. Security Evaluations
    3. Parameters Documented Within PSP for Operation

Thank you

Chris Chwasz - INL

Alan Evans - SNL