U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

13.6.1 PHYSICAL SECURITY—COMBINED LICENSE AND OPERATING REACTORS

REVIEW RESPONSIBILITIES

Primary: Organization responsible for the review of physical security.

Secondary: Licensing organization and cognizant review organization according to the standard review plan (SRP) sections identified in the attached sample final safety analysis report (FSAR) Table 13.4-x for integrated review of safety and security in design.

I. AREAS OF REVIEW

This section provides guidance for the review of combined construction and operating license (COL) and operating license (OL) applications and amendments for physical security. The staff reviews include the design of engineered physical security systems, hardware, and features (hereinafter referred to as "physical security systems" or PSS), the administrative controls (hereinafter referred to as "operational requirements") and management systems (program, policies, processes, procedures) for operations and organization within the scope of a COL or OL application. The scope of the U.S. Nuclear Regulatory Commission (NRC) staff review

Draft Revision 2 – April 2017

includes the descriptions used to establish the licensing bases for acceptance of the licensee's physical protection program; the information required to address the design, construction, and installation of PSS; and the implementation of operational requirements, management systems, and organization for meeting the performance and prescriptive requirements of Title 10, "Energy," of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials." The areas of review also include topical or technical reports incorporated by reference as part of the COL application (COLA). The NRC staff's review of the applicant's or licensee's bases should consider how all regulatory requirements will be met to support a finding of whether the Commission should grant a request for an operating license or an amendment to a license in accordance with the standards and criteria set forth for the Commission in 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and Subpart C, "Combined Licenses," of 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

The requirements of 10 CFR Section 52.79, "Contents of Applications; Technical Information in Final Safety Analysis Reports," in particular 10 CFR 52.79(a)(35)(i) and (ii) and 10 CFR 52.79(a)(36)(i) through (v), require that an applicant (or a licensee) must meet all applicable requirements in 10 CFR Part 73. The requirements to meet 10 CFR Part 26, "Fitness for Duty Programs," are in 10 CFR 52.79(a)(44). Under 10 CFR 52.79(a)(35) and 52.79(a)(36), which incorporate by reference 10 CFR Part 73, COL applicants are required to prepare plans that describe a physical protection program (engineered systems and administrative controls) that will be constructed, installed, and implemented to protect their facilities against acts of radiological sabotage. After issuance of a COL, the COL holder (i.e., licensee) is required to implement a physical protection program that maintains the licensing bases described in the application and captures the engineered and administrative controls, management systems, and organization described for operating a nuclear power plant to include meeting all applicable regulatory requirements.

The requirements of 10 CFR Part 50 establish the procedures and criteria for issuing construction permits and for licensing production and utilization facilities. The requirements in 10 CFR 50.33, "Contents of Applications; General Information," and 10 CFR 50.34, "Contents of Applications; Technical Information," establish applications' requirements for a utilization facility construction-permit. The regulations in 10 CFR 50.34 require applicants to submit a preliminary safety analysis report that addresses site-evaluation factors identified in 10 CFR Part 100,"Reactor Site Criteria," and contains summary descriptions and discussions of the facility (10 CFR 50.34(a)(2)) and preliminary plans for organization, training, and conduct of operations. An FSAR and security plans (10 CFR 50.34(c)(1) through 10 CFR 50.34(c)(3), 10 CFR 50.34(d), and 10 CFR 50.34(e)) are included in an application for an OL.

The licensing processes defined in 10 CFR Parts 50 and 52 form the regulatory basis for the staff's technical review of physical protection for a nuclear power reactor based on the requirements of 10 CFR Part 73. Therefore, the NRC staff guidance described in this SRP applies to reviewing both license applications and license amendments for nuclear power reactors that have applied for or been issued a license under either of the licensing processes described in 10 CFR Parts 50 and 52.

The NRC staff's review consists of the following:

(1) Confirm that the engineered and administrative controls, management systems, and organization described in licensing documents adequately address the performance and prescriptive requirements of 10 CFR Part 73 and remain consistent with guidance provided in NRC Regulatory Guide (RG) 1.206, "Combined License Applications for Nuclear Power Plants (LWR [Light-Water Reactor] Edition)," for a new reactor license application. Where applicable, under 10 CFR Part 52, the licensing documents address the interface with the COLA. The reviewer may accomplish this by examining any COL information items necessary to address the designs of physical security systems and physical security hardware - inspections, tests, analyses, and acceptance criteria (PS-ITAAC) to include site-specific or COL-specific information, along with the descriptions of programs, management systems, and organization that are outside the scope of a cited certified design or standard design.

2. The guidance in RG 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)," addresses the requirement of 10 CFR 50.34 regarding a preliminary safety analysis report (PSAR). Each application for a license to operate such a facility includes an FSAR. Regulations in 10 CFR 50.34 specify the general terms of the information to be supplied in these safety analysis reports (SARs). The principal purpose of the SAR is to inform the Commission of the nature of the plan, the plans for its use, and the safety evaluations that have been performed to evaluate if the plant can be constructed and operated without undue risk to the public health and safety. The SAR is the principal document for the applicant to provide information needed to understand the basis on which the NRC reached its conclusion about public health and safety. The SAR is also the principal document cited in the construction permit or operating license and is the basic document used by NRC inspectors to determine if the facility is being constructed and operated within the licensed conditions. The staff reviews include reviews of the FSAR (i.e., Part 2 of the license application) and other parts of the application (e.g., Parts 1, 7, 8, 10, etc.) that may be applicable to how the licensee will meet regulatory requirements of 10 CFR Part 73.

3. The security licensing bases are described in the security plan (Part 8 of the license application), which consists of the physical security plan (PSP), training and qualification plan (T&QP), and the safeguards contingency plan (SCP) and is provided in FSAR Chapter 13, "Conduction of Operations," Section 13.6, "Security." However, because the security plan contains Safeguards Information (SGI) as defined in 10 CFR 73.21, "Protection of Safeguards Information," the security plan is provided separately in Part 8 of the license application to protect SGI from public disclosure. Section 13.6 of the FSAR incorporates the information provided in the security plan to establish the licensing bases for how the applicant (or a licensee) plans to secure the operations of a nuclear power plant.

4. The staff's review includes review of the interfaces with the cited certified or standard design, design related to the early site permit or construction permit, site characteristics that must be considered in providing physical security. The interfaces necessary to ensure that the review (i.e., as secondary reviewer) of information addressed under other NUREG-0800 includes descriptions of plant structures, systems, and components,

operational requirements, and management systems that are credited with providing physical security functions and implementation of operational and management systems for a physical security program.

Scope of the Technical Review for Physical Security

1. At a minimum, information contained in licensing documents must be sufficiently detailed to demonstrate how performance and prescriptive requirements of 10 CFR Part 73 will be met. The scope of technical review includes key standards and criteria for the design of, and operational requirements for, physical protection set forth in 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," along with other applicable sections of 10 CFR Part 73. The reviewer should use the information provided as licensing bases, which include engineering controls (i.e., PSS) and administrative controls (operational requirements) for the design of a physical protection system (i.e., detection, assessment, communications, and response for interdiction and neutralization), to determining how a an applicant (or a licensee) meets the performance requirement of 10 CFR 73.55(b) to protect against the DBT for radiological sabotage. The information also includes details on management systems and organizations.

2. The application must provide information that is sufficiently detailed to demonstrate how regulatory requirements for procurement, construction, and installation of PSS are met and how operational requirements for physical protection systems provide protection against the design-basis threat (DBT) of radiological sabotage as established by the performance and prescriptive design requirements of 10 CFR 73.55(b). The scope includes the descriptions of the design bases for PSS that are relied on by the physical protection system and the descriptions of administrative controls and management systems that address operational requirements, training and qualification of personnel, and safeguards contingency planning. This information establishes the licensing bases for the physical protection program and provides the bases for the Commission's determination of whether a nuclear power plant would be adequately protected and operated in accordance with NRC regulatory requirements.

3. As stated in SECY-11-0024, "Use of Risk Insights To Enhance the Safety Focus of Small Modular Reactor Reviews," dated February 18, 2011 (available as Agencywide Documents Access and Management System (ADAMS) Accession No. ML111320551), the level of review for a particular structure, system, or component (SSC) is derived from both the SSC's safety importance (i.e., whether the SSC is safety-related or nonsafety-related) and risk significance. NUREG-0800, Introduction - Part II, Revision 0, describes the licensing review framework the NRC staff applies for new reactor design certification and combined license applications under 10 CFR Part 52 or operating license applications processed under 10 CFR Part 50. The introduction states that the risk-informed review framework is applicable to the review of all SSCs, but it may not apply to the review of programmatic, procedural, organizational, or other topics, which, because of their safety or risk significance, are reviewed at the level determined to be appropriate by the technical branches performing the reviews. For example, the program or topical area may address regulatory requirements not amenable to a risk-informed approach (e.g., physical protection for safety of nuclear material and

operations, waste management, and instruments and control systems). In the case of physical security, the review framework involves performance and prescriptive regulatory requirements that do not incorporate risk significance and address protection (against deliberate acts such as radiological sabotage) and prescriptive design requirements. However, the safety significance of adequate technical review for physical security is the assurance of adequate protection against deliberate acts, which are not specifically considered or analyzed in the FSAR. Therefore, the technical review ensures that the risks for operating a nuclear power plant are acceptable and within the safety envelope and environmental protection standards and criteria analyzed and may be implemented in accordance with requirements and conditions of the license.

4. For COL and OL applications, the staff reviews the security plans, (which consist of the PSP, T&QP, and SCP) submitted under Part 8 of the COL or OL application. These plans describe all elements and components of the physical protection program, such as the security organization, security equipment and technology, the performance-evaluation program; the insider mitigation program; the access-authorization program; and the fitness-for-duty (FFD) program, safety and security interface processes, the cyber security program, and the proposed implementation milestones. The scope of review also includes information in Part 2, of a COLA or OL application and the descriptions of the physical protection program (e.g., FSAR Section 13.6), along with required licensing conditions for implementation of physical protection programs.

5. For COL or OL applicants that do not cite a certified or standard design, or where specific designs of physical protection system are reserved for a COL applicant, the staff will review the descriptions of the PSS and their associated design basis under SRP Section 13.6.2, “Physical Security—Design Certification.” This section establishes the scope of the technical review pertaining to designs and performance requirements of PSS within the nuclear island structures, PA (protected area), and OCA (owner-controlled area).

6. Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC):

   A. Specific to a COLA, the staff review includes the applicant’s proposed ITAAC in accordance with SRP Section 14.3, “Inspections, Tests, Analyses, and Acceptance Criteria.” The review of PS-ITAAC is performed in accordance with guidance provided in NUREG-0800 SRP Section 14.3.12, “Physical Security Hardware—Inspections, Tests, Analyses, and Acceptance Criteria,” to confirm that the PS-ITAAC, including test abstracts and proposed management systems, are identified and addressed appropriately within the design certification (DC) application for a standard design and within the COL application, as needed, to address site-specific designs of engineered physical security systems. The review and documentation of the evaluation of site-specific PS-ITAAC are not within the scope of review described in this SRP.

   B. ITAAC as described above are not requirements for an OL under 10 CFR Part 50. Therefore, the review of PS-ITAAC is not within the scope of an OL application. Under 10 CFR 50.34(c)(2), 50.34(d)(2), an applicant or licensee

must describe how regulatory requirements will be met and operational readiness review inspections may be imposed by the Commission as a condition of license for an OL issued under the provisions of 10 CFR 50.50, “Issuance of Licenses and Construction Permits.”

7. COL Information Items, Certification Requirements, and Restrictions:

   A. Specific to a COLA, the staff technical review will include the review of how the COL information items, requirements, and restrictions (e.g., interface requirements and site parameters established during an early site permit described in a DC or a standard design) are addressed.

   B. The staff reviewer should confirm that specific design descriptions are that addressed by a COL applicant citing a certified or standard design meet prescriptive requirements. The COL applicant must satisfactorily describe how it will meet all applicable regulatory requirements. Additionally, a COL applicant must address the applicable interface and site parameter requirements and restrictions that may be established in NRC-approved early site permits.

Review Interfaces

Other SRP sections interface with this section in these ways:

1. The descriptions related to the design of PSS performing security functions are found in the cited certified design or standard design. The FSAR for the COLA and OL application contains site-specific information that may have security significant. Review interfaces may be based on the applicant’s approach to the design of engineered systems, operational requirements, and management systems for the conduct of operations meeting security functions and requirements. For example, plant lighting systems may provide multiple functions that satisfy both safety and security requirements and may not necessarily be designed as a dedicated system for the sole purpose of providing or supporting only a security or a safety (i.e., a single) function. Also, Chapter 13, “Conduct of Operations,” of the FSAR addresses management systems that are applicable to the conduct of security operations and the management of the safety and security interface for plant operations.

2. The staff that has primary or lead review responsibilities, as indicated in the applicable SRP sections, will review the adequacy of the SSC’s designs, operational requirements, and management measures. The secondary reviewers provide assurance that the interfaces are addressed when the SSC’s designs, operational requirements, and management systems are intended to perform multiple functions (i.e., safety, security, environmental protection, plant infrastructures, work controls, configuration management, the corrective-action program, etc.).

3. The review of interfaces includes how the proposed design and specifications meet the applicable performance and prescriptive regulatory requirements. The review should also include operational requirements and management systems and should confirm that they satisfy regulatory requirements.

4. These topical or subject areas establish or require the review interfaces:

   A. NUREG-0800, SRP 1.0, Introduction and Interfaces (all review organizations are assigned secondary review responsibilities)

   B. NUREG-0800, SRP 2.0, Sites Characteristics and Site Parameters

   C. NUREG-0800, SRP 8.1, Electric Power—Introduction

   D. NUREG-0800, SRP 8.3.1, A-C Power Systems (Onsite)

   E. NUREG-0800, SRP 8.3.2, D-C Power Systems (Onsite)

   F. NUREG-0800, SRP 9.5.2, Communications Systems

   G. NUREG-0800, SRP 9.5.3, Lighting Systems

   H. NUREG-0800, SRP 13.6.2, Physical Security—Design Certification

   I. NUREG-0800, SRP 13.6.4, Access Authorization Operational Program

   J. NUREG-0800, SRP 13.6.6, Cyber Security Plan

   K. NUREG-0800, SRP 13.7.1, Fitness for Duty—Operational Program

   L. NUREG-0800, SRP 13.7.2, Fitness for Duty—Construction

   M. NUREG-0800, SRP 14.3.12, Physical Security Hardware—Inspections, Tests, Analyses, and Acceptance Criteria

The above-cited SRP sections contain the specific acceptance criteria and review procedures.

II. ACCEPTANCE CRITERIA

Requirements

The NRC bases the acceptance criteria on meeting the relevant requirements of the following Commission regulations:

1. 10 CFR Part 52, Subpart C, “Combined Licenses,” Section 52.79, “Contents of Applications; Technical Information in Final Safety Analysis Reports,” 10 CFR 52.79(a)(35)(i) and (ii) and 10 CFR 52.79(a)(36)(i) through (v), which require that an applicant or licensee meet all applicable requirements in 10 CFR Part 73.

2. 10 CFR 52.80(a), which requires that a COL application contain the proposed ITA, including those applicable to emergency planning which the licensee shall perform, and also contain the acceptance criteria necessary and sufficient to provide reasonable assurance that if the ITA are performed and the acceptance criteria are met, the facility

will have been constructed and will operate in conformance with the COL, the provisions of the Atomic Energy Act of 1954 (as amended), and NRC regulations. The certified design (i.e., rule), in part, provides the portion of the final design and specification of physical security systems and associated ITAAC that are incorporated by reference in a COL application to meet this requirement.

3. Where a COL or an OL cites a certified design, 10 CFR Part 52, Subpart B, "Standard Design Certification," Section 10 CFR 52.47, "Contents of Applications; Technical Information," identifies required design information specific to standards set out in 10 CFR Part 73. The designs of physical security systems, along with their design bases, within a certified design are incorporated by reference and therefore not included in the scope of the COL or OL licensing review.

4. 10 CFR 50.33 and 10 CFR 50.34 define the requirements for applying for a construction permit for a utilization facility, which include a preliminary safety analysis report that address site-evaluation based on requirements of 10 CFR Part 100,"Reactor Site Criteria," with summary descriptions and discussions of the facility (10 CFR 50.34(a)(2)), a preliminary plan for organization, training, and conduct of operations and an FSAR and security plans (10 CFR 50.34(c)(1) through 10 CFR 50.34 (c)(3), 10 CFR 50.34(d), and 10 CFR 50.34(e)) for each operating license (OL).

5. 10 CFR 73.1, "Purpose and Scope," which requires the establishment and maintenance of physical security capable of protecting plants in which special nuclear material is used; defines radiological sabotage and the attributes, assistance, and equipment of the DBT (including attributes related to land and waterborne vehicle bomb assault, internal threat, and cyber-attack).

6. 10 CFR 73.2, "Definitions," which defines terms relevant to physical security, including those applicable to physical security systems, operational requirements, and management systems (e.g., "bullet-resisting," "physical barriers," "intrusion alarm," "lock," "protected area," "vital area," "vital equipment," "isolation zone," etc.). The provisions of 10 CFR 73.3, "Interpretations," states that only a written interpretation by the NRC General Counsel will be recognized as binding upon the Commission.

7. 10 CFR 73.4, "Communications," which identifies specific requirements for filing applications and sets forth requirements for communications and reports concerning physical security regulations.10 CFR 73.5, "Specific Exemptions," as it relates to specific exemptions to regulatory requirements identified in 10 CFR Part 73. The requirements of 10 CFR 50.12 and 10 CFR 52.7, both also titled "Specific Exemptions," set forth the criteria by which the Commission may grant exemptions to requirements of regulations under 10 CFR Part 50 and 10 CFR Part 52, respectively, and how they apply to an exemption to the requirements of 10 CFR Part 73.

8. 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements," and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements," as they relate to requirements on any person who produces, receives, or acquires SGI; identify specific requirements to protect against unauthorized disclosure; describe information

that should be protected; and identify requirements for storage, transport, and controls that must be implemented and maintained to protect SGI for a nuclear reactor license.

9. 10 CFR 73.55, beginning with 10 CFR 73.55(a), “Introduction,” which identifies the licensee’s responsibility to implement “security plans” and written security implementing procedures; requires applicants and licensees to implement the requirements of 10 CFR 73.55 before fuel is allowed onsite (in the protected area (PA)); places specific requirements on Tennessee Valley Authority (TVA) Watts Bar Nuclear Plant, Unit 2; and states that the requirements of Section 73.55(i)(4)(iii) must be met by applicants for an OL, or holders of a COL, that do not cite a standard DC or cites a standard DC issued after May 26, 2009.

10. 10 CFR 73.55(b), “General Performance Objective and Requirements,” which specifies the performance-based regulatory requirement that facilities be protected against the DBT of radiological sabotage; requires that a physical protection program be designed to maintain the capability to detect, assess, interdict, and neutralize threats up to the DBT of radiological sabotage; requires defense in depth (DID) through the integration of systems and technologies; and defines the objective of the security organization as being to provide high 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.

11. 10 CFR 73.55(c), “Security Plans,” as it relates to describing how requirements in 10 CFR Part 73 will be implemented through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, the implementation of predetermined response plans and strategies, and the protection of digital computer and communication systems and networks.

12. 10 CFR 73.55(d), “Security Organization,” as it relates to establishing and maintaining a security organization that is designed, staffed, trained, qualified, and equipped to implement the physical protection program in accordance with requirements in Section 10 CFR 73.55, including those found in Appendix B and C to 10 CFR Part 73.

13. 10 CFR 73.55(e), “Physical Barriers,” as it relates to identifying and analyzing site-specific conditions to determine the specific use, type, function, and placement of physical barriers needed to satisfy the physical protection program design requirements of 10 CFR 73.55(b). including prescriptive requirements of physical barriers in 10 CFR 73.55(e)(1) through 10 CFR 73.55(e)(10).

14. 10 CFR 73.55(f), “Target Sets,” as it relates to documenting and maintaining the process used to develop and identify target sets, to include the site-specific analyses and methodologies used to determine and group the target set equipment or elements..

15. 10 CFR 73.55(g), “Access Controls,” as it relates to the control personnel, vehicle, and material access, as applicable, at each access control point in accordance with the physical protection program design requirements of § 73.55(b).

16. 10 CFR 73.55(h), “Search Programs,” as it relates to establishing a search program to detect, deter, and prevent the introduction of firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage through search of individuals, vehicles, and material consistent with the physical protection program design requirements in 10 CFR 73.55(b), and the function to be performed at each access control point or portal. ;

17. 10 CFR 73.55(i), “Detection and Assessment Systems,” as it relates to establishing and maintaining intrusion detection and assessment systems that satisfy the design requirements of 10 CFR 73.55(b) and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the effective implementation of the site protective strategy.

18. 10 CFR 73.55(j), “Communication Requirements,” as it relates to establishing and maintaining continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

19. 10 CFR 73.55(k), “Response Requirements,” as it relates to the establishing and maintaining, at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threat up to and including the design basis threat of radiological sabotage as defined in 10 CFR 73.1, to prevent significant core damage and spent fuel sabotage.

20. 10 CFR 73.55(l), “Facilities Using Mixed-Oxide (MOX) Fuel Assemblies Containing up to 20 Weight Percent Plutonium Dioxide (PuO_2)*,”* as it relates to the additional requirements described in this section to protect un-irradiated MOX fuel assemblies against the theft or diversion, through: (a) administrative controls; (b) physical controls; (c) staffing; (d) capability to detect, assess, interdict and neutralize threats; and (d) Commission approval for MOX fuel assemblies great than 20 weight percent PuO_2.

21. 10 CFR 73.55(m), “Security Program Reviews,” as it relates to the licensee’s review elements of the physical protection program, including the requirements for reviews, scope of reviews, documentation, and tracking and resolution of findings.

22. 10 CFR 73.55(n), “Maintenance, Testing, and Calibration,” as it relates to the establishing, maintaining, and implementing maintenance, testing, and calibration programs to ensure the security systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions. .

23. 10 CFR 73.55(o), “Compensatory Measures,” as it relates to identifying criteria and measures to compensate for degraded or inoperable equipment, systems, and components to meet requirement of 10 CFR 73.55.

24. 10 CFR 73.55(p), “Suspension of Security Measures,” as it relates to criteria and requirements for suspension of security measures in accordance with 10 CFR 50.54(x) and 50.44(y) or during severe weather, reinstating suspended security measures, and

reporting of such suspensions in accordance with the requirements of 10 CFR 73.71, "Reporting of Safeguards Events."

25. 10 CFR 73.55(q), "Records," as it relates to maintaining 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 maintaining superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the Commission.

26. 10 CFR 73.55(r), "Alternative Measures," as it relates to alternative protection measures; criteria for authorization of such measures; submission of proposed alternative measures for review and approval, including full descriptions of the change and its technical basis and demonstrating an equal level of protection; specific requirements for alternative vehicle barrier systems (VBS); and cost considerations.

27. 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants," as it relates to requirements for establishing, implementing, and maintaining personnel access-authorization requirements.

28. 10 CFR 73.57, "Requirements for Criminal History Records Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility, a Non-Power Reactor, or Access to Safeguards Information," as it relates to requirements for submitting fingerprints for those individuals who will access to safeguards information and for those individuals who will require unescorted access to the nuclear power facility.

29. 10 CFR 73.58, "Safety/Security Interface Requirements for Nuclear Power Reactors," as it relates to managing the safety and security interface for planned and emergent activities for conduct of plant operations, including communicating potential conflict and take compensatory and/or mitigate actions to maintain safety and security.

30. 10 CFR 73.70, "Records," as it relates to records, their content and type of information (particularly records of specific security information, shipment of special nuclear material (SNM), and access-control procedures), and their retention requirements.

31. 10 CFR 73.71, "Reporting of Safeguards Events," as it relates to notifying the NRC Operations Center within one hour to report safeguards events, including the recipients and timing of notification, information reported, submission of written reports, and minimum criteria for reporting.

32. Section VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," of Appendix B, "General Criteria for Security Personnel," to 10 CFR Part 73, as it relates to establishing and following plans for selecting, training, equipping, testing, and qualifying individuals for security-related duties and responsibilities.

33. Section I, "Safeguards Contingency Plans," of Appendix C, titled "Licensee Safeguards Contingency Plans," Section to 10 CFR Part 73, as it relates to establishing a

safeguards contingency plan to define the licensee's objectives in its response to events of threats, thefts, or radiological sabotage.

34. Appendix G, "Reportable Safeguards Events," to 10 CFR Part 73, as it relates to the types of safeguards events that must be reported by any means within 1 hour (and in writing within 60 days) and the types of safeguards events that must be recorded within 24 hours in the safeguards event log.

SRP Acceptance Criteria

The documents listed in this section provide criteria that the NRC finds acceptable for meeting the relevant requirements of the agency's regulations identified above. This SRP is not a substitute for NRC regulations, and compliance is not required. The acceptance criteria delineated in this SRP are intended to communicate the underlying objectives. Rather, an applicant should tailor its security program to the site-specific conditions and features of its nuclear reactor. However, the NRC requires an applicant to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria. The NRC also requires an applicant or licensee to evaluate how any proposed alternatives to the SRP acceptance criteria provide acceptable methods of compliance with NRC regulations. The staff retains the responsibility to make an independent determination concerning the adequacy of the applicant's or licensee's proposed approaches.

The following RGs, NUREGs, and industry standards provide guidance related to the design of physical security systems. In general, they describe methods or approaches and technical bases that may be applied for meeting the requirements described above:

1. U.S. Nuclear Regulatory Commission, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plant (LWR Edition)," Regulatory Guide 1.70, ADAMS Accession No. ML011340122.

2. U.S. Nuclear Regulatory Commission, "Combined License Application for Nuclear Power Plants (LWR Edition)," Regulatory Guide 1.206, available at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/rg/01-206/.

3. U.S. Nuclear Regulatory Commission, "Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas," Regulatory Guide 5.7, ADAMS Accession No. ML003739976.

4. U.S. Nuclear Regulatory Commission, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials," Regulatory Guide 5.12, ADAMS Accession No. ML003740035.

5. U.S. Nuclear Regulatory Commission, "Perimeter Intrusion Alarm Systems," Regulatory Guide 5.44, ADAMS Accession No. ML003739217.

6. U.S. Nuclear Regulatory Commission, "Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants," Regulatory Guide 5.54, ADAMS Accession No. ML13151A355, not publicly available.

7. U.S. Nuclear Regulatory Commission, “Vital Area Access Controls, Protection of Physical Security Equipment, and Key and Lock Controls,” Regulatory Guide 5.65, ADAMS Accession No. ML003739336.

8. U.S. Nuclear Regulatory Commission, “Protection Against Malevolent Use of Vehicles at Nuclear Power Plants,” Regulatory Guide 5.68, ADAMS Accession No. ML003739379.

9. U.S. Nuclear Regulatory Commission, “Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements” (as it relates to the design of physical security systems), Regulatory Guide 5.69, ADAMS Accession No. ML13151A355, not publicly available.

10. U.S. Nuclear Regulatory Commission, “Cyber Security Programs for Nuclear Facilities,” Regulatory Guide 5.71, ADAMS Accession No. ML090340159.

11. U.S. Nuclear Regulatory Commission, “Managing the Safety/Security Interface,” Regulatory Guide 5.74, ADAMS Accession No. ML091690036.

12. U.S. Nuclear Regulatory Commission, “Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities,” Regulatory Guide 5.75, ADAMS Accession No. ML091690037.

13. U.S. Nuclear Regulatory Commission, “Physical Protection Programs at Nuclear Power Reactors,” Regulatory Guide 5.76, ADAMS Accession No. ML13151A355, not publicly available.

14. U.S. Nuclear Regulatory Commission, “Insider Mitigation Program,” Regulatory Guide 5.77, ADAMS Accession No. ML13151A355, not publicly available.

15. “Target Set Identification and Development for Nuclear Power Reactors,” Regulatory Guide 5.81, ADAMS Accession No. ML13151A355, not publicly available.

16. U.S. Nuclear Regulatory Commission, “High Security Protected and Vital Area Barrier/Equipment Penetration Manual,” Regulatory Issue Summary 2003-06, not publicly available.

17. U.S. Nuclear Regulatory Commission, “Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants,” *Federal Register*, Vol. 50, No. 153, August 8, 1985, pp. 32138–32150, ADAMS Accession No. ML003711521.

18. NUREG-1959, “Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees,” NUREG-1959, March 2011, ADAMS Accession No. ML11112A009.

19. U.S. Nuclear Regulatory Commission, “Access Control Systems: Technical Information for NRC Licensees,” NUREG-1964, April 2011, ADAMS Accession No. ML11115A078.

20. “Vehicle Barriers: Emphasis on Natural Features,” NUREG/CR-4250, July 1985.

21. "Entry/Exit Control Components for Physical Protection Systems," NUREG/CR-5899, November 1992.

22. U.S. Nuclear Regulatory Commission, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants: Vehicle Barrier System Siting Guidance for Blast Protection," NUREG/CR-6190, Vols. 1 and 2, Rev. 1, December 1994; the two volumes are available at www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA325232 and www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA326506 respectively.

23. U.S. Nuclear Regulatory Commission, "Nuclear Power Plant Security Assessment Guide," NUREG/CR-7145, April 2013, ADAMS Accession No. ML13122A181.

24. U.S. Department of Energy, Sandia National Laboratories, "Technology Transfer Manuals," not publicly available:

- SAND99-2388, "Interior Intrusion Detection"
- SAND99-2389, "Video Assessment"
- SAND99-2390, "Alarm Communication"
- SAND99-2391, "Exterior Intrusion Detection"
- SAND99-2392, "Protecting Secure Communications"
- SAND99-2486, "Explosives Protection"
- SAND2000-2142, "Entry Control and Contraband Detection Systems"
- SAND2001-2168, "Access Delay Technology," Volume 1

25. U.S. Department of Defense, "Structures to Resist the Effects of Accidental Explosions"; United Facilities Criteria (UFC) 3-340-02, December 2008, available at http://www.wbdg.org/ccb/DOD/UFC/ufc_3_340_02.pdf.

26. U.S. Department of Justice, National Institute of Justice, "Ballistic Resistant Protective Materials," NIJ Standard 0108.01, September 1985, available at http://www.ncjrs.gov/pdffiles1/nij/099859.pdf.

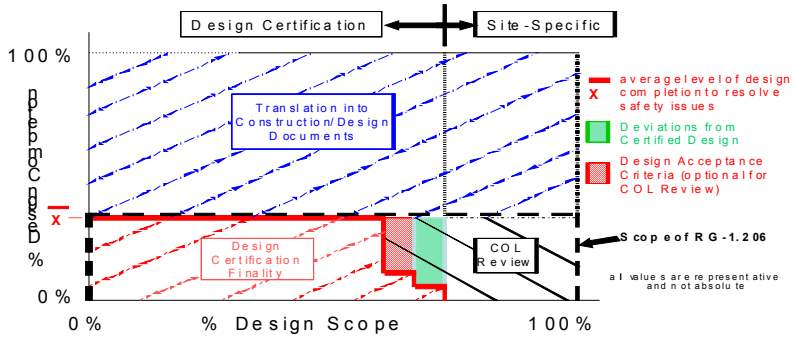
27. Underwriters Laboratories, Inc., "Standard for Bullet-Resisting Equipment," UL 752, September 2005.

The applicant may apply or describe and identify other references and technical guidance for the designs of physical security systems that apply technical approaches, methods, or technologies that are based on sound and fundamental principles of science and engineering and that provide defensible technical bases for the proposed equivalent or alternative designs, operational requirements, or management systems for meeting the regulatory requirements in Section II.

In general, the detail for the design of a physical protection system is acceptable when the proposed design of engineered and administrative controls, management systems, and organization specifically describes how the performance and prescriptive design criteria in 10 CFR 73.55 will be met. The NRC bases acceptability on how a physical security program,

including a physical protection system, provides reliability and availability (i.e., through diversity, independence, and separation, as applicable, and DID) of engineered and administrative controls. Information pertaining to the reliability and availability of a system (integrated engineered and administrative controls) for performing the intended security function should demonstrate that the system (as described) will achieve —or facilitate achieving—the general performance and requirements of 10 CFR 73.55(b) and the prescriptive requirements applicable to a nuclear power reactor in 10 CFR Part 73.

Based on the guidance in RG 1.206, the descriptions for the design of physical security systems satisfy the requirements when the design descriptions provide sufficient detail that conforms to the guidance for the design scope and descriptions for design completion in Figure 1, "Combined License Application Referencing a Certified Design," shown below.



Combined License Application Referencing a Certified Design

The completeness and accuracy of information required for an application and the adequacy of the level of detail, however, is determined by whether the applicant's licensing bases are sufficiently described for the NRC staff to make regulatory findings that: (1) all applicable regulatory requirements will be met, (2) there is reasonable assurance that the facility will be constructed and will operate in conformity with the license, the provisions of the Atomic Energy Act of 1954 (as amended), and the Commission's regulations, and (3) there is reasonable assurance that issuance of the license will not be inimical to the common defense and security or to the health and safety of the public, to justify granting the request for a COL or OL or an amendment to the license.

The staff acceptance is based on meeting regulatory requirements in 10 CFR Part 73 and conforming to applicable and associated review acceptance criteria for the designs of the specific physical security systems, operational requirements, and management systems. The applicant's descriptions should address in sufficient detail how the required engineered and administrative controls and management systems are designed, organized, and conducted to enable the reviewer to understand the capabilities and functions that will be established, maintained, and implemented for the physical protection of the nuclear power reactor

In most cases, descriptions provided by the applicant that are confirmatory statements or restatements of regulatory requirements and that do not provide sufficient descriptions and do not illustrate or demonstrate how the engineered and administrative controls and management systems will satisfy the performance or prescriptive regulatory requirement and conform to SRP acceptance criteria will not be acceptable for satisfying the requirements of 10 CFR Parts 50 and 52 for licensing. However, some regulatory requirements may be sufficiently prescriptive that their use in the applicant's description will sufficiently describe how the requirement must be met (e.g., where the regulation defines an explicit configuration, specific times or quantities of weight, specific dimensions, exact type of material for constructions). The descriptions must provide a sufficient level of detail about the proposed physical security systems within the design for the Commission to determine that all applicable regulatory requirements will be met. They also must include the details of how physical security systems will be designed, constructed, and installed and how operational requirements and management systems will be established, maintained, and implemented to perform required security functions.

The descriptions must provide sufficient details in the security plans, along with the FSAR, for the Commission to determine that all applicable regulatory requirements will be met and that the licensing bases for the physical security of an operating nuclear power plant are clearly established, will be maintained, and can be implemented. Descriptions stating only that detail for how regulatory requirements will be met and will be provided in implementing procedures or can be found in implementing procedures are not acceptable descriptions of how regulatory requirements will be met and, therefore, do not provide adequate licensing bases for findings regarding reasonable assurance for the Commission's issuance of a COL, an OL, or a license amendment. Although detailed procedures are not required to be submitted for NRC review, the applicant or licensee clearly describes the licensing bases for how procedures will address regulatory requirements; how procedures will implement management measures and define the conduct of security operations; how those procedures will be established; how those procedures will be maintained and revised and how those revisions will be controlled. These descriptions of the licensing bases provide, in part, the reasonable assurance that, if they are implemented as described, regulatory requirements will be met and the conduct of operations involving special

nuclear material will not be inimical to the common defense and security and will not constitute an unreasonable risk to the public health and safety.

The format and content of the security plan may conform to the most recent revision of the NRC-accepted Nuclear Energy Institute (NEI) 03-12, "Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Program]." A security plan conforming to NEI 03-12 is considered acceptable if it contains sufficiently detailed information addressing how all regulatory requirements will be met, captures the licensing bases for a physical protection program which meets the performance and prescriptive requirements set forth in 10 CFR Part 73, and supports the overall reasonable assurance safety finding that the issuance of a license and operations will not be an unacceptable risk to public health and safety, an unacceptable risk to the environment, or inimical to common defense and security.

Specific SRP Acceptance Criteria

The information below provides the specific SRP acceptance criteria for the design of engineered controls, operational requirements, and management systems (programs, processes, procedures, etc.). The acceptance criteria are established based on regulatory requirements and are listed in the order that they appear in 10 CFR Part 73. The staff should only apply the acceptance criteria as applicable to the scope of review for the requested operating license, amendment to a license, alternative measure, or a specific exemption.

1. 10 CFR 73.1 is satisfied when the following standards and criteria against radiological sabotage and for protection of a nuclear power reactor are met:

   A. protection against violent external assaults and methods (10 CFR 73.1(a)(1))

   B. protection against assailants who are well-trained and dedicated, willing to kill or be killed, knowledgeable, active, and equipped (10 CFR 73.1(a)(1)(i)(A) through 10 CFR 73.1(a)(1)(i)(E))

   C. protection against internal threats, land-vehicle bomb assaults, waterborne-vehicle bomb assaults, and cyber-attacks (10 CFR 73.1(a)(1)(ii) through 10 CFR 73.1(a)(1)(v))

2. 10 CFR 73.2 is satisfied when specific terms in an applicant's descriptions of security licensing bases and information docketed for an application are defined the same way as they are in the regulation: "armed escort"; "armed response personnel"; "authorized individual"; "background check"; "bullet/resisting"; "contiguous site"; "continuous visual surveillance"; "deceit"; "force"; "guard"; "incendiary device"; "individual authorized access to safeguards information"; "intrusion alarm"; "isolation zone"; "need to know"; "person"; "physical barrier"; "safeguards information"; "security management"; "security supervisor"; "special nuclear material of low strategic significance"; "tactical response team"; "transport"; "trustworthiness"; "vital area"; "vital equipment"; and "watchman" (10 CFR 73.2(a), 10 CFR 73.2(a)(1), 10 CFR Part 50, and 10 CFR Part 52).

3. 10 CFR 73.21 and 10 CFR 73.22 are satisfied when descriptions of engineered controls, operational requirements, and management systems provide sufficient details about how safeguards information will be protected:

   A. protection against unauthorized disclosure (10 CFR 73.21(a)(1))

   B. establishment, implementation, and maintenance of an information protection system (i.e., processes and procedures) that safeguards the information specified in 10 CFR 73.22 as it applies to power reactors (10 CFR 73.21(a)(1)(i) and 73.21(a)(1)(iii))

   C. application of information-protection procedures employed by the U.S NRC, which are acceptable for meeting requirements for protection against unauthorized disclosure (10 CFR 73.21.(a)(2))

   D. specific requirements for protection of safeguards information, including the determination of which information is to be protected; physical protection in transit; inspections, audits, and evaluations; and correspondence (10 CFR 73.22(a))

   E. restricting access to safeguards information based on the need to know the information and using background checks to gauge personnel trustworthiness and reliability (10 CFR 73.22(b))

   F. protection of safeguards information while it is being used or stored (10 CFR 73.22(c))

   G. preparation and marking of safeguards information (10 CFR 73.22(d))

   H. reproduction of safeguards information (10 CFR 73.22(e))

   I. external transmission and transport of safeguards information (10 CFR 73.22(f))

   J. processing of safeguards information on electronic systems (10 CFR 73.22(g))

   K. removal of the “safeguards information” designation (10 CFR 73.22(h))

   L. destruction of safeguards information (10 CFR 73.22(i))

4. 10 CFR 73.55(a) is satisfied when descriptions of engineered controls, operational requirements, and management systems, as well as organization descriptions, provide sufficient details to meet these criteria, including specifying a schedule for program implementation:

   A. Each nuclear power reactor licensed under 10 CFR part 50 has revised its Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Cyber Security Plan referred to collectively hereafter as ‘‘security

plans.' to describe how the requirements of 10 CFR 73.55 will be met, by March 31, 2010. (10 CFR 73.55(a)(1)).

B. Current applicants for an operating license under 10 CFR part 50, or combined license under 10 CFR part 52 who have submitted their applications to the Commission prior to the effective date [March 10, 2010] of this rule must amend their applications to include security plans,(10 CFR 73.55(a)(1)).

C. The security plan identifies and describes in sufficient detail how site-specific conditions are accounted for in meeting the requirements of 10 CFR 73.55 and identifies the organization responsible for maintaining a physical protection program and implementing security plans and written procedures (10 CFR 73.55(a)(2) and 10 CFR 73.55(a)(3)). The site-specific conditions include the site characteristics, including parameters and any restrictions to or impediments on developing security plans (as addressed in a referenced early site permit or construction permit, if applicable).

D. A specific license condition is provided for the implementation of a reactor security program (in accordance with the requirements of 10 CFR 73.55 and all applicable sections of 10 CFR Part 73) for a nuclear power reactor before fuel is allowed onsite (in the protected area) for an operating license issued under the provisions of 10 CFR Part 50 or a combined license issued under the provisions of 10 CFR Part 52.

E. The TVA Watts Bar Nuclear Plant, Unit 2, holding a current construction permit under the provisions of 10 CFR Part 50, shall meet the revised requirements in paragraphs (a) through (r), as applicable to the descriptions of physical security required to meet the requirements for a construction permit under the provision of 10 CFR Part 50 (10 CFR 73.55(a)(5)).

F. Applicants for an OL or COL that do not cite a standard design certification at all or that cite a standard design certification issued after May 26, 2009 shall meet the requirement of 10 CFR 73.55(i)(4)(iii), which addresses equal and redundant alarm stations and required functions (10 CFR 73.55(a)(6)).

5. 10 CFR 73.55(b) is satisfied when engineered controls, operational requirements, management systems, and organization descriptions provide sufficient details about how performance requirements will be met based on the following criteria:

A. Establish and maintain a physical protection program, to include a security organization, which will have as its objectives to (1) provide high 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 and (2) protect against the DBT of radiological sabotage, specifically to prevent significant core damage and spent fuel sabotage (10 CFR 73.55(b)(1) and (2)).

B. Establish and maintain a physical protection program to prevent significant core damage and spent fuel sabotage, following the criteria set forth in 10 CFR 73.55(b), including 73.55(b)(i) and (ii):

(i) 10 CFR 73.55(b)(3)(i) is satisfied when the applicant adequately describes how the designs of physical security systems, operational requirements, and management systems provide the capabilities to detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage. To meet the performance-based regulatory requirements, the applicant determines and proposes how it will provide or design a physical protection system (i.e., a system for detection, assessment, communications, delay, and security response) that will protect a nuclear power plant and its nuclear operations against the DBT of radiological sabotage resulting from significant core damage or loss of spent fuel pool cooling. The requirement of 10 CFR 73.55(b)(3)(ii), as it relates to the design of physical protection systems (PSS), is satisfied when design descriptions include how PSS will be designed and how operational requirements (administrative controls) will be integrated to address how each element of a physical protection system contributes to the system's capability to detect, assess, communicate, and respond (interdict and neutralize). It includes the design and specifications of engineered and administrative controls addressing the reliability and availability of PSS that are providing or are relied on by the administrative controls (i.e., people and procedures) to deliver high assurance of detection, assessment, interdiction, and neutralization. Therefore, the descriptions should address each element of a PPS and must meet the requirements of 10 CFR 73.55(b)(i) and (b)(ii), as they relate to the design of a physical protection system.

(ii) At a minimum, the detailed licensing bases should address the issues described in paragraphs i through vi below to satisfy the performance requirements of 10 CFR 73.55(b)(i) and (b)(ii) using engineered and related operational requirements for physical security. The information submitted must be sufficient to complete detailed design for procurement, construction, and installation of physical security systems and detailed administrative controls (outlining required staffing, equipment, and procedures) that meet regulatory requirements.

a) *Interior and Exterior Intrusion Detection and Assessment:* The descriptions of designs and specifications should be of sufficient detail to establish, but not limit, the following for engineered physical security systems providing intrusion detection and assessment: (1) types of systems, their applications, and intended functions; (2) installation and location of systems and subsystems, including specific areas of coverage; (3) configurations of major structures, systems, and subsystems and their locations and systems interfaces; (4) configurations and protection of electrical and alarm signal transmission lines; (5) electrical power sources

addressing primary power, secondary power, and uninterruptable power supply; (6) lighting specifications required for detection and assessment; (7) systems monitoring and human interfaces; and (8)the technical basis for, and the specifications of, the protection that these systems provide against particular characteristics of the DBT.

b) *Security Communications for Initiating Security Response for Interdiction and Neutralization:* The descriptions of designs and specifications should be of sufficient detail to establish, but not be limited to, the following for engineered physical security systems providing security communications: (1) types of systems and their applications and intended functions; (2) installations and locations; (3) configurations of major structures, systems, and components and their locations and interfaces; (4) protecting communication signals; (5) electrical power sources addressing primary power, secondary power, and uninterruptable power supply; (6) redundancy for protection against DBT characteristics affecting availability of security communications; and (7) the technical basis for, and the specifications of, the protection that these systems provide against particular characteristics of the DBT..

c) *Physical Barriers, Delay Systems, and Features Relied on for Interdicting and Neutralizing DBT:* The descriptions of designs and specifications should be of sufficient detail to establish, but not be limited to, the following for engineered physical security systems providing minimum physical delays times: (1) design and configurations of active and passive engineered systems, types of material, their applications, and intended functions; (2) installations and locations of the engineered passive and active barrier systems; (3) configurations of major structures, systems, and components and their interfaces; (4) electrical power sources addressing primary power, secondary power, and uninterruptable power supply or primary and secondary mechanical or fluid motor forces for active engineered systems; (5) physical dimensions and topographical characteristics, including special distances, which are relied on as delay features; (6) safety/security interfaces for impact on nuclear operations and safety; and (7) the technical basis for, and the specifications of, the protection that these systems provide against particular characteristics of the DBT.

d) *Physical Security Systems Relied on for Interdiction and Neutralization:* The descriptions of designs and specifications should be of sufficient detail to establish, but not be limited to, the following for engineered physical security systems or features relied on for protection of security responders to provide tactical advantage over DBT adversaries for interdiction and

neutralization: (1) design and configurations of active and passive engineered systems, types of material, their applications, and intended functions; (2) installations and locations of the engineered passive and active barrier systems; (3) configurations of major structures, systems, and components and their interfaces; (4) configurations and protection of electrical, alarm, data, and control signal transmission lines; (5) electrical power sources addressing primary power, secondary power, and uninterruptable power supply or primary and secondary mechanical or fluid motor forces for active engineered systems; (6) lighting specifications required for performing neutralization; (7) technical basis and specifications of DBT characteristics protected; and (8) safety and security interfaces impacting both nuclear and non-nuclear safety and conduct of operations.

e) *Physical Security Systems for Interdiction and Neutralization:* The descriptions of designs and specifications should be of sufficient detail to establish, but not be limited to, the following for engineered physical security systems providing neutralization functions: (1) types of systems, their applications, and intended functions; (2) installations and locations of systems and subsystems, including specific areas of coverage; (3) configurations of major structures, systems, and subsystems and their locations and systems interfaces; (4) configurations and protection of electrical, alarm, data, and control signal transmission lines; (5) electrical power sources addressing primary power, secondary power, and uninterruptable power supply; (6) camera and lighting specifications for interdiction and neutralization; (7) systems monitoring and human factors for human-machine interfaces; (8) redundancy for protection against DBT characteristics affecting availability of security communications; (9) safety and security interfaces for impact on nuclear operations, safety, or emergency response; and (10) technical basis for and the specifications of the DBT characteristics that are protected.

f) *Defense-in-Depth Designs of Physical Security Systems and Operational Requirements (Security Response):* The designs of physical security systems should address systems diversity, independence, and separation, for defense-in-depth to achieve a high assurance of intended security functions and must meet all specific prescriptive design criteria set forth in 10 CFR 73.55. Defense-in-depth is an element of the NRC's philosophy that is used to address uncertainty by using successive measures, including safety margin, to prevent and mitigate damage if a malfunction, accident, or natural caused event occurs at a nuclear facility. Defense-in-depth philosophy applies to measures against intentional acts as required by 10 CFR 73.55(b). The most

common defense-in-depth measures apply concepts of redundancy, diversity, independences, 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 (i.e., provide high assurance that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety). Redundancy is to achieve system reliability through the use of independent means of accomplishing needed function (i.e., ensuring no single failure results in loss of the intended function). Diversity and separation provide protection against dependent (common cause) failures of multiple means of accomplishing needed functions. Diversity is achieved by using different technologies, equipment, manufacturers, control logic, signals, and functions to provide a diverse way of accomplishing the intended security function. Independence is attained by physical separation and physical barriers, including electrical or motor force independence. Operational requirements (i.e., security responses providing interdiction and neutralization functions) provide DID by using layers of protection that include diverse, separate, and independent armed responders 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 system, which integrate engineered controls and administrative controls, to provide a high assurance of protection against the DBT for radiological sabotage.

C. 10 CFR 73.55(b)(4) is satisfied when sufficient details (summary and conclusions capturing security-significance requirements) of analyses and consideration of site-specific conditions are addressed in the design of the physical protection program. The summary and results of target sets are provided in sufficient details to demonstrate what must be protected and how the physical protection program meets the performance requirements of 10 CFR 73.55(b)(1) through 73.55(b)(ii).

D. 10 CFR 73.55(b)(5) is satisfied when sufficient details of management systems (e.g., processes and procedures) are provided to determine how a performance evaluation program will be established, maintained, and implemented in accordance with the regulatory requirements of Appendix C to 10 CFR Part 73. The details should be sufficient as to how the PSP will specifically verify the demonstration of and the assessment of the effectiveness of armed responders and armed security officers in implementing the licensee's protective strategy (i.e., how the PSP protects against the DBT).

E. 10 CFR 73.55(b)(6) through 73.55(b)(9) are satisfied when descriptions of engineered controls, operational requirements, and management systems provide sufficient details of how these programs will be established, maintained, and implemented in accordance with regulatory requirements:

(i) a personnel access-authorization program in accordance with 10 CFR 73.56

(ii) a cyber-security program in accordance with 10 CFR 73.54

(iii) an insider mitigation program described in sufficient detail and containing program elements from the access-authorization program, fitness-for-duty program (10 CFR Part 26), cyber security program, and physical protection program (10 CFR 73.55) that meets criteria for: (a) initial and continued monitoring for trustworthiness, (b) ensuring the reliability of individuals granted or retaining authorization for unescorted access to a protected or vital area, and (c) implementing defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the capability to prevent significant core damage and spent fuel sabotage.

F. 10 CFR 73.55(b)(10) and 10 CFR 73.55(b)(11) are satisfied when the descriptions of the management system (i.e., processes) provide sufficient details of how the plant's corrective-action program will be applied to track, trend, correct, and prevent recurrence of failures and deficiencies in the physical protection program, and how management systems will coordinate security plans and procedures to preclude conflict during both normal and emergency operating conditions (i.e., how the safety/security interface will be managed).

6. 10 CFR 73.55(c) is satisfied when the security plans (consisting of a PSP, T&QP, SCP, and CSP) describe in sufficient details the engineered and administrative controls, management systems, and organization required to meet the following criteria:

A. Security plans describe how the licensee will implement requirements of 10 CFR 73.55 through a security organization, the use of security equipment and technology, the training and qualification of security personnel, the implementation of predetermined response plans and strategies, and the protection of digital computer and communication systems and networks (10 CFR 73.55(c)(1)(i)).

B. Security plans address site-specific conditions that affect how the licensee implements Commission requirements (10 CFR 73.55(c)(1)(ii)).

C. The licensee protects security plans and other security-related information from unauthorized disclosure in accordance with requirements of 10 CFR 73.21 (10 CFR 73.55(c)(2)).

D. A PSP describes in sufficient detail how the performance objective and requirements set forth in 10 CFR 73.55(b) will be established, maintained, and implemented (10 CFR 73.55(c)(3)).

E. A T&QP describes in sufficient detail how the requirements set forth in Section VI of Appendix B to 10 CFR Part 73 will be established, maintained, and implemented (10 CFR 73.55(c)(4)).

F. An SCP describes in sufficient detail how the requirements set forth in Section II of Appendix B to 10 CFR Part 73 will be established, maintained, and implemented (10 CFR 73.55(c)(5)).

G. An CSP describes in sufficient detail how the requirements set forth in 10 CFR 73.54 will be established, maintained, and implemented (10 CFR 73.55(c)(6)).

H. A management system describes in sufficient detail (related to security implementing procedures) how these criteria will be met:

(i) Describe how procedures implementing regulatory requirements of 10 CFR Part 73 will be developed, implemented, revised, and reviewed (10 CFR 73.55(c)(7)(i)).

(ii) Document the security organization's structure and details of the types of duties, responsibilities, actions, and decisions to be performed or made by each position of the security organization (10 CFR 73.55(c)(7)(ii)).

(iii) Establish a process for written approval and revision of implementing procedures with overall responsibility for the physical protection program that satisfies the requirements of 10 CFR 73.55 (10 CFR 73.55(c)(7)(iii)(A) and (B)).

(iv) Implementing procedures are available for inspection (10 CFR 73.55(c)(7)(iv)).

7. 10 CFR 73.55(d) is satisfied when the applicant describes in sufficient detail how a security organization will be established, maintained, designed, staffed, trained, qualified, and equipped to implement the requirements of 10 CFR 73.55, and includes attributes meeting these criteria:

A. The security organization establishes a management system for overseeing implementation of the physical protection program and provides at all times, onsite, at least one security organization member who has the authority to direct the activities of the security organization and who is assigned no other duties that would interfere with his or her ability to perform these duties as described in the security plans (10 CFR 73.55(d)(2)(i) and 73.55(d)(2)(iii)).

B. The management system prohibits any individual from implementing 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 Section VI of Appendix B to 10 CFR Part 73 (10 CFR 73.55(d)(3)).

C. A management system ensures that non-security personnel, if assigned duties and responsibilities required to implement the physical protection program: (1) are trained, qualified, and periodically requalified to perform the assigned duties, (2) are properly equipped to perform the assigned duties, and (3) have the knowledge, skills, and abilities, including physical attributes such as adequate sight and hearing, required to perform their assigned duties and responsibilities.

8. 10 CFR 73.55(e) (see SRP Section 13.6.2), contains requirements that relate to the design, use, types, functions, and placement of physical barriers to satisfy the capabilities and the design descriptions provide sufficient detail of how the construction and installation of the physical barrier systems address prescriptive design criteria. The requirements related to the operational requirements and management systems of 10 CFR 73.55(e) are satisfied when the applicant describes in sufficient detail how operational requirements and management systems will meet these criteria:

A. securing and monitoring of openings and penetrations to prevent their exploitation (10 CFR 73.55(e)(4) and 73.55(e)(8)(ii))

B. monitoring, detection, and assessment of intrusion (10 CFR 73.55(e)(7)(i)(B) and 73.55(e)(7)(i)(C))

C. locating obstructions that could prevent the licensee from meeting observation and assessment requirements outside the isolation zone (10 CFR 73.55(e)(7)(ii))

D. allowing prompt egress during an emergency and satisfying requirements for access control into the protected area and vital areas (10 CFR 73.55(e)(8)(iii) and 73.55(e)(9)(ii))

E. periodically checking exterior areas within the protected area to detect and deter unauthorized personnel, vehicles, and material (10 CFR 73.55(e)(8)(v))

F. periodically checking the operations of an active vehicle barrier system, and providing a secondary power source or a means of mechanical or manual operation, to ensure that the active barrier can be placed in the denial position (10 CFR 73.55(e)(10)(i)(B))

G. periodic surveillance and observation of vehicle barrier systems to detect indication of tampering and degradation in order to ensure that the systems can perform their intended function (10 CFR 73.55(e)(10)(i)(C))

H. periodic surveillance of rail access-control measures (10 CFR 73.55(e)(10)(i)(D))

I. identifying areas from which waterborne vehicles are restricted and coordinating with local, State, and Federal agencies having jurisdiction over waterway approaches (10 CFR 73.55(e)(10)(ii)(A))

J. periodic surveillance and observation of waterway approaches and adjacent areas (10 CFR 73.55(e)(10)(ii)(B))

9. 10 CFR 73.55(f) is satisfied when the applicant describes in sufficient detail how the operational requirements and management system will meet these criteria:

A. Document and maintain the process, analyses, and methodologies used to develop and identify target sets (10 CFR 73.55(f)(1)).

B. The process includes consideration of cyber-attack (10 CFR 73.55(f)(2)).

C. Identify and document target-set equipment or elements that are not contained within a protected or vital area and how they are accounted in the site-protective strategy provided to against the DBT (10 CFR 73.55(f)(3)).

D. The process for overseeing and documenting changes to target sets' equipment and systems is accounted for in requirements for physical protection (10 CFR 73.55(f)(4)).

10. 10 CFR 73.55(g) (see SRP Section 13.6.2), as it relates to the design of access control measures required to protect against the threats up to and including the DBT of radiological sabotage, addresses the criteria specific to the design and performance of physical security systems for access control. The requirements that relate to the operational requirements and management systems of 10 CFR 73.55(g) are satisfied when the applicant describes in sufficient detail how operational requirements and management systems will meet these criteria:

A. Provide supervision and control over the badging process to prevent unauthorized bypass of access-control equipment (10 CFR 73.55(g)(1)(i)(C)).

B. Limit unescorted access to protected and vital areas, during nonemergency (10 CFR 73.55(g)(1)(i)(D)).

C. Assign an individual the responsibility for last access-control function and response (10 CFR 73.55(g)(1)(i)(E)).

D. Grant and control access, search for contraband, and observe search functions at vehicle barriers (10 CFR 73.55(g)(1)(ii)(A) through 73.55(g)(1)(ii)(C)).

E. Confirm identity, verify authorization for access, confirm any denial of access, and search individuals accessing the protected area (10 CFR 73,55(g)(2)(i) through 73.55(g)(2)(iv)).

F. Control the access of all vehicles operated by individuals authorized for escorted or unescorted access, limit use of vehicles to plant functions or emergencies, remove keys or disable vehicles when not in use, and provide armed escort of hazardous material transport (10 CFR 73.55(g)(3)(i) through 73.55(g)(3)(iv)).

G. Control access to vital areas with access-authorization lists and implementation of the two-person (line-of-sight) rule for vital areas in response to site-specific credible threat (10 CFR 73.55(g)(4)(i) and 73.55(g)(4)(ii)).

H. Address potential needs during emergencies or conditions leading to emergencies for rapid ingress or egress by authorized individuals and implement security procedures to give authorized emergency personnel prompt access to affected areas and equipment (10 CFR 73.55(g)(5)(i) and 73.55(g)(5)(ii)).

I. Control all keys, locks, combinations, passwords, and related access-control devices used to reduce the probability of compromise by taking these actions:

(i) Issue access-control devices only to individuals with unescorted and required access (10 CFR 73.55(g)(6)(i)(A)).

(ii) Maintain records (10 CFR 73.55(g)(6)(i)(B)).

(iii) Implement compensatory measures upon discovery or suspicion of a compromised access device until the compromise is corrected (10 CFR 73.55(g)(6)(i)(C)).

(iv) Retrieve, change, rotate, deactivate, or otherwise disable access-control devices that have been or may have been compromised or when a person with access to control devices has been unfavorably terminated (10 CFR 73.55(g)(6)(i)(D)).

(v) Implement controls for use of a numbered photo identification badge system for all individuals authorized unescorted access to the protected and vital areas, including conditions for removal of badges from the protected area, display of badges on one's person, and records of badge recipients. (10 CFR 73.55(g)(6)(ii) through 73.55(g)(6)(ii)(C)).

(vi) Issue passwords and combinations to personnel in the access-authorization program (10 CFR 73.55(g)(6)(iii).

(vii) Implement controls and procedures for processing, escorting, and controlling visitors; confirming their identity; maintaining a visitor control register; issuing visitor badges; and establishing conditions for denying escorted access (10 CFR 73.55(g)(7) through 73.55(g)(7)(i)(F)).

(viii) Implement requirements for individuals performing escort duties, including means of timely communication with security personnel for assistance, training and qualification, knowledge of activities for reporting unusual

behavior or activities, and visitor-to-escort ratios. (10 CFR 73.55(g)(8) through 73.55(g)(8)(v)).

11. 10 CFR 73.55(h) (see SRP Section 13.6.2), including 10 CFR 73.55(h)(3)(i) and 73.55(h)(2)(v), as it relates to the design of search-system equipment and configuration (and where required, design of video-surveillance equipment), addresses the criteria specific to the design and performance of physical security systems for searches. The requirements that relate to operational requirements and management systems of search programs in 10 CFR 73.55(h) to detect, deter, and prevent the introduction of firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage are satisfied when the applicant describes in sufficient detail how operational requirements and management systems will meet these criteria:

    A. Implement search procedures for access-control points at established barriers in the owner-controlled area that identify areas of a vehicle to be searched (which must include, but are not limited to, the cab, engine compartment, undercarriage, and cargo area); search items; perform searches with at least two individuals, one of whom is positioned to observe the search process and provide immediate response; perform vehicle searches (1) using equipment capable of detecting firearms, explosives, incendiary devices, or other items that can be used for sabotage, or (2) through visual and physical searches, or (3) both; and equip vehicle access control points with video-surveillance equipment monitored by an individual capable of initiating a response (10 CFR 73.55(h)(2) through 73.55(h)(2)(v)).

    B. Implement search procedures for all personnel, vehicles, and material requesting access to the protected area, including: searching for firearms, explosives, incendiary devices, or other items through the use of equipment or through visual and physical searches or both; subjecting all persons except official Federal, state, and local law enforcement personnel on official duty to searches; permitting armed security officers on duty who have exited the protected area to re-enter the protected area without being searched for firearms; performing visual and physical searches whenever search equipment is unavailable or not reliable; implementing actions in response to attempts to introduce contraband to deny access and perform assessment of threat; and describing in implementing procedures the areas of vehicles to be searched (10 CFR 73.55(h)(3) through 73.55(h)(3)(iv)).

    C. Grant exceptions based on safety or operational reasons to searches of materials brought into the protected area only under conditions established and documented in the security plans and site procedures, provided that the requirements of 10 CFR 73.55(b) are satisfied (10 CFR 73.55(h)(3)(v)).

    D. Positively control excepted materials, store them in a locked area, and have an individual familiar with them open the materials at the final destination. Bulk material excepted from search requirements must have an armed escort and shall not be offloaded adjacent to a vital area (10 CFR 73.55(h)(3)(vi) and 73.55(h)(3)(vii)).

12. 10 CFR 73.55(i) (see SRP Section 13.6.2), as it relates to how the design of detection and assessment systems, which satisfy the design requirement of 10 CFR 73.55(b) and provide at all times the capability to detect and assess unauthorized access and facilitate the implementation of security response) addresses criteria in 10 CFR 73.55(i)(1) through 73.55(i)(6) to satisfy the requirements of 10 CFR 73.55(b). The requirements that relate to operational requirements and management systems of 10 CFR 73.55(i) are satisfied when the applicant describes in sufficient detail how operational requirements and management systems will meet these criteria:

    A. Continuously staff each alarm station with at least one trained and qualified alarm station operator and do not assign them duties or responsibilities that would interfere with their function as an alarm station operator; assess and initiate response to all alarms and other events as appropriate; ensure that operators at both stations are knowledgeable of the final disposition of all alarms; and maintain records of all alarm annunciation, causes, and dispositions (10 CFR 73.55(i)(4)(ii)(B), (D), (E), (G), and (H)).

    B. Perform surveillance, observation, and monitoring as needed for meeting the requirements of 10 CFR 73.55(b), including identifying tampering; detect intruders and ensure the integrity of physical barriers or other components for security functions; and perform continuous surveillance, observation, and monitoring by security personnel during continuous patrols, by using video technology, or by doing a combination of both (10 CFR 73.55(i)(5)(i) and (ii)).

    C. Perform surveillance, observation, and monitoring of unattended openings that intersect a security boundary, including underground pathways protected by a physical barrier and monitored by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation (10 CFR 73.55(i)(5)(iii)).

    D. Perform checks and inspections by armed security patrols of external areas of the protected area and vital areas, including physical barriers at vital-area portals, and perform random patrols of all accessible areas containing target-set equipment (10 CFR 73.55(i)(5(iv) through (vi)).

    E. Train security personnel to recognize obvious indications of tampering in a way consistent with their assigned duties and responsibilities; initiate a security response to detection of tampering or other threats (10 CFR 73.55(i)(5)(vii) and (viii)).

    F. Illuminate the facility, as needed, to meet the requirements of 10 CFR 73.55(b). Either provide at least 0.2 foot-candles of illumination or augment the lighting system with low-light technology, documenting the types and applications of such technology and how it meets lighting requirements (10 CFR 73.55(i)(6)(i) through (iii)).

13. 10 CFR 73.55(j) (see SRP Section 13.6.2), as it relates to how the design of physical security systems or plant systems providing communications that satisfy the requirement of 10 CFR 73.55(b) and meet prescriptive design criteria. The requirements that relate to operational requirements and management systems of 10 CFR 73.55(j) are satisfied when the applicant describes in sufficient detail how operational requirements and management systems will meet these criteria:

    A. Continuous communication capability with onsite and offsite resources ensures command and control during normal and emergency operations (10 CFR 73.55(j)(1)).

    B. Individuals in each alarm station shall be capable for calling for assistance (10 CFR 73.55(j)(2)).

    C. All on-duty security force personnel shall be capable of maintaining continuous communication with an individual in each alarm station; vehicle escorts shall maintain timely communication with security personnel (10 CFR 73.55(j)(3)).

    D. Implementing procedures shall account for site areas where communications could be interrupted or cannot be maintained (10 CFR 73.55(j)(4)).

14. 10 CFR 73.55(k), as it relates to how response requirements satisfy the performance requirement of 10 CFR 73.55(b) and provide, at all times, the capability to respond to attempted radiological sabotage, is satisfied when the applicant describes in sufficient detail how it will address these criteria:

    A. Operational requirements are integrated with specific technologies (e.g., fixed or deployable fighting positions, remotely operated weapon systems, etc.), and described in the PSP, to protect responders and/or provide capabilities to interdict and neutralize adversaries (10 CFR 73.55(k)(1)).

    B. A sufficient supply of working and readily available firearms, munitions, and equipment is provided to implement the security plan (10 CFR 73.55(k)(2)).

    C. Armed security personnel are trained to respond with sufficient force, including use of deadly force that is justified in self-defense or in the defense of others, or under other circumstances authorized by applicable State or Federal law. (10 CFR 73.559(k)(3)).

    D. Armed security personnel (armed responders and armed security officers) can carry out response duties within predetermined timelines established and required by the design of a physical protection system (i.e., the protective strategy to detect, assess, communicate, delay, and interdict/neutralize threats) (10 CFR 73.55(k)(4)).

    E. The minimum number of armed responders required to satisfy 10 CFR 73.55(b) and implement the response (to interdict and neutralize threats) of the protective strategy is not less than ten; all required armed responders are available at all

times inside the PA and are not assigned duties and responsibilities that would interfere with their response duties (10 CFR 73.55(k)(5)(i) through (iii)).

F. The number of armed security officers required to implement the protective strategy is documented; the security officers are onsite and available at all times to carry out response duties (10 CFR 73.55(k)(6)(i) and (ii)).

G. Procedures exist to reconstitute the documented number of available armed response personnel (10 CFR 73.55(k)(7)).

H. The licensee shall establish, maintain, and implement a written protective strategy in accordance with the 10 CFR 55 and Appendix C to 10 CFR Part 73, including a management system for receiving indication of threats, determining the level of threats, initiating responses, and notifying local law enforcement, as appropriate for the level of threat (10 CFR 73.55(k)(8)(i) through (iii)).

I. Establish and maintain agreements with law enforcement agencies, including estimated response times and capabilities (10 CFR 73.55(k)(9)).

J. Establish, maintain, and implement a threat warning system with specific graduated protective measures and actions (10 CFR 73.55(k)(10)).

15. 10 CFR 73.55(l) is satisfied when descriptions for designs of physical security systems, operational requirements, and management systems provide sufficient details of how the use of MOX fuel assemblies containing up to 20 weight percent PuO_2 will be protected in accordance with these criteria:

A. Administrative controls and management systems for receipt, inspection, movement, storage, and protection of un-irradiated MOX fuel assemblies are described in the security plan, and include the use of tamper-indicating devices, inspections for damage, searches for unauthorized materials, proper placement and control (i.e., at least one armed security officer present for inspection, storage of MOX fuel assemblies only in a spent fuel pool), and a material and accounting program (10 CFR 73.55(l)((3)).

B. Specific controls to lock, lockout, or disable all equipment and power supplies to equipment required for movement and handling of un-irradiated MOX fuel assemblies; implementation of a two-person rule; minimum presence of one armed security officer; use of security officers knowledgeable about authorized and unauthorized activities involving un-irradiated MOX fuel assemblies; performance of required surveillance; and continuous capability to detect, assess, and neutralize threats to the fuel assemblies (10 CFR 73.55(l)(4)(i), (4)(ii), (4)(v)(A) through (4)(v)(C), (5), and (6)).

C. Requests to use MOX fuel assemblies containing greater than 20 weight percent PuO_2 shall be approved by the Commission before the assemblies are received; additional measures to protect such assembles shall be determined by the

Commission on a case-by-case basis and documented through license amendment (10 CFR 73.55(l)(7)).

16. 10 CFR 73.55(m) is satisfied when descriptions of operational requirements, management systems, and organization provide sufficient details to describe the licensing bases for how security program reviews will be implemented, along with required documentation and reporting in accordance with these criteria:

    A. Review each element of the physical protection program at least every 24 months and within 12 months after initial implementation or changes to personnel, procedures, equipment, or facilities that could adversely affect security or (10 CFR 73.55(m)(1) through 73.55(m)(1)(ii)).

    B. Have individuals independent of direct responsibility for implementing the physical security program conduct the review (10 CFR 73.55(m)(1)(iii)).

    C. Reviews must include an audit of the effectiveness of the program; security plans; implementing procedures; cyber security programs; the safety/security interface; the testing, maintenance, and calibration program; and offsite response (10 CFR 73.55(m)(2)).

    E. Document review results, recommendations, findings, and resulting actions taken in a report to plant and corporate management that is auditable and available for inspection (10 CFR 73.55(m)(3)).

    F. Enter findings from reviews into the site's corrective action program (10 CFR 73.55(m)(4)).

17. 10 CFR 73.55(n) is satisfied when descriptions of operational requirements, management systems, and organization provide sufficient details to describe how the maintenance, testing, and calibration program for physical security systems and equipment relied on to meet security functions will meet these criteria:

    A. Establish, maintain, and implement a maintenance, testing, and calibration program; describe it in the physical security plan; specify in implementing procedures such maintenance, testing, and calibration details as the purpose of the activity, the actions to be taken, the criteria for acceptance, and the intervals at which the activity will be performed; and determine when to document problems, failures, deficiencies, and other findings; and intervals (10 CFR 73.55(n)(1)(i) through 73.55(n)(1)(iv)).

    B. Implement compensatory measures for failure or degraded operation (10 CFR 73.55(n)(1)(v)).

    C. Conduct specific performance and operability tests of intrusion-detection, access-control, communications, and search equipment at minimum specified frequencies (10 CFR 73.55(n)(2) through 73.55(n)(6)).

D. Specify in implementing procedures a program for testing or verifying operability of devices or equipment located in hazardous areas and test security equipment before returning it to service after a repair or from an inoperable condition (10 CFR 73.55(n)(7) and 73.55(n)(8)).

18. 10 CFR 73.55(o) is satisfied when descriptions of operational requirements, management systems, and organization provide sufficient details to identify criteria and measure to compensate for degraded or in-operable equipment, systems and components and describe the licensing bases for how compensatory measures will meet the following::

    A. Compensatory measures must provide a level of protection equivalent to that was provided by the degraded or inoperable equipment, systems, or components (10 CFR 73.55(o)(2)).

    B. Compensatory measures must be implemented within the specific time frames necessary to meet the requirements of 10 CFR 73.55(b) and described in the security plans (10 CFR 73.55(o)(3)).

19. 10 CFR 73.55(p) is satisfied when descriptions of operational requirements, management systems, and organization provide sufficient details to describe the licensing bases for how suspension of affected security measures implementing the requirements of 10 CFR 73.55 will meet the following criteria:

    A. In accordance with 10 CFR 50.54(x) and 50.54(y), in an emergency or during severe weather, suspend security measures only if there is an immediate need to protect public health and safety and no action consistent with license conditions and technical specifications is immediately apparent to provide adequate or equivalent protection. The suspension of security measures must be approved as a minimum, by , a licensed senior operator, with input from the security supervisor or manager (10 CFR 73.55(p)(1)(i) and (ii)).

    B. Suspended security measure must be reinstated as soon as conditions permit (10 CFR 73.55(p)(2)).

    C. Suspension of security measures must be reported and documented in accordance with the requirements of 10 CFR 73.71 (10 CFR 73.55(p)(3)).

20. 10 CFR 73.56 is satisfied when descriptions for operational requirements, management systems, and organization provide sufficient details to describe the licensing bases for how requirements for personnel access to a nuclear power plant will meet the criteria in 10 CFR 73.56(a) through 73.56(o). The review of access authorization is outside the scope of this SRP section; see staff guidance described in SRP 13. 6.4 for staff technical review of access authorization and RG 5.66, “Access Authorization Program for Nuclear Power Plants,” for acceptable methods and approaches for meeting regulatory requirements.

21. 10 CFR 73.57 is satisfied when descriptions for operational requirements, management systems, and organization provide sufficient details to describe how to comply with the requirements for addressing criminal history checks of individuals granted unescorted access or access to SGI applicable to an applicant. This would include submitting fingerprints for those individuals who will require unescorted access and meeting the prescriptive criteria set forth in the remainder of 10 CFR 73.57(a) through 10 CFR 73.57(g).

22. 10 CFR 73.58 is satisfied when descriptions for operational requirements, management systems, and organization provide sufficient details to describe the licensing bases for how requirements for managing the safety and security interface meet the following criteria:

    A. Assess and manage the potential for adverse effects on safety and security before implementing changes to plant configurations, facility conditions, or security before implementation (10 CFR 73.58(b)).

    B. The changes assessed and managed must include planned and emergent activities (10 CFR 73.58(c)).

    C. Where potential conflicts are identified, the licensee shall communicate them to appropriate personnel and take compensatory and/or mitigating actions to maintain safety and security under Commission regulations, requirements, and conditions of license (10 CFR 73.55(d)).

23. 10 CFR 73.70 is satisfied when sufficient details describe how operational requirements and management systems will establish records of information that are legible, accurate, and complete; in the proper format; stored properly for the, required period of retention; and protected by safeguards against tampering and loss of records and content to meeting the following criteria:

    A. The licensee shall retain the names and addresses of all individuals designated as authorized individuals for the period during which the licensee possesses the appropriate type and quantity of special nuclear material that is subject to the recordkeeping requirement and for 3 years thereafter. Copies of superseded material must be retained for three years after each change (10 CFR 73.70(a)).

    B. The licensee shall retain the names, addresses, and badge numbers of all individuals authorized to have access to vital equipment or special nuclear material, and the designations of the vital areas to which authorization is granted, for the period during which the licensee possesses the appropriate type and quantity of special nuclear material that is subject to the recordkeeping requirement and for 3 years thereafter. Copies of superseded material must be retained for 3 years after each change (10 CFR 73.70(b)).

    C. The licensee shall maintain a register of visitors, vendors, and other individuals not employed by the licensee under 10 CFR 73.55(d)(6), and shall retain this

register as a record for 3 years after the last entry is made in the register (10 CFR 73.70(c)).

D. The licensee shall maintain a log indicating the name, badge number, time of entry, and time of exit of all individuals granted access to a vital area except those individuals entering or exiting the reactor control room, and shall retain this log as a record for 3 years after the last entry is made in the log (10 CFR 73.70(d)).

E. The licensee shall document all routine security tours and inspections and all tests, inspections, and maintenance performed on physical barriers, intrusion alarms, communications equipment, and other security-related equipment used under the requirements of 10 CFR 73.70, and shall retain the documentation for these events for 3 years from the date of documenting each event (10 CFR 73.70(e)).

F. The licensee shall maintain a record at each onsite alarm-annunciation location of each alarm, false alarm, alarm check, and tamper indication that identifies the type of alarm, location, alarm circuit, date, and time. In addition, details of response by facility guards and watchmen to each alarm, intrusion, or other security incident shall be recorded. The licensee shall retain this record for 3 years after the record is made (10 CFR 73.70(f)).

G. The licensee shall document its procedures for controlling access to protected areas and for controlling access to keys for locks used to protect special nuclear material, shall retain a copy of the current procedures as a record until the Commission terminates each license for which the procedures were developed, and shall retain any superseded portion of the procedures for 3 years after each change (10 CFR 73.70(g)).

24. 10 CFR 73.71(b) is satisfied when descriptions of the operational requirements, management systems, and organization provide sufficient details to describe how requirements for reporting of safeguards events meet the criteria of notifying the NRC Operations Center within 1 hour of discovery of the safeguards events described in paragraph I(a)(1) of Appendix G to 10 CFR Part 73; how notification is made in accordance with the requirements specified for the Emergency Notification System; how an open and continuous communication channel is maintained; how the initial notification is followed by a written report within 60 days; and how supplemental information is provided (10 CFR 73.75(a)(1) through (5), 73.75(b)(1) and (2), and 73.75(c) through (e)).

25. Section VI of Appendix B to 10 CFR Part 73 (as it relates to requirements for selecting, training, equipping, testing, and qualifying individuals who are responsible for the protection of special nuclear materials, nuclear facilities, and nuclear shipments, and other personnel who perform security duties), is satisfied when descriptions for the operational requirements, management systems, and organization provide sufficient details about how these types of requirements will be met: (1) general requirements, (2) employment suitability and qualifications, (3) duty training, (4) duty qualification and

requalification, (5) the weapon qualification and requalification program; (6) weapons, personnel equipment, and maintenance and (6) records.

26. Section II of Appendix C to 10 CFR Part 73, as it relates to preparedness and the safeguards contingency plan, is satisfied when the descriptions of the operational requirements and organization provide sufficient details about how requirements are met for: (1) a safeguards contingency plan to organize response effort, predetermined response, integrations of response, and achieving measurable performance, (2) the content of the plan addresses its background, generic planning bases, licensing planning bases, responsibility matrix, and implementing procedures, and (3) records and reviews associated with the plan.

27. Sections I and II of Appendix G to Part 73, as it relates to reportable safeguards events, is satisfied when the descriptions for the operational requirements and organization provide sufficient details about how requirements are met for: (1) events to be reported within one hour of discovery and then in a written report within 60 days and (2) events to be reported within 24 hours of discovery in the safeguards event log.

28. Conditions of License

    For COL applications, the NRC reviews the description of the operational program and the proposed implementation milestone(s) for the physical security program in accordance with 10 CFR 73.55; for the security training and qualification program, in accordance with Sections VI.A through VI.I of Appendix B to 10 CFR Part 73; and for the safeguards contingency response program, in accordance with Section II of Appendix C to 10 CFR Part 73; for the access-authorization program, in accordance with 10 CFR 73.56; for the FFD program, in accordance with 10 CFR Part 26. The implementation milestone for the completion of all operational programs in this section is before fuel is allowed onsite (inside the protected area) unless a specific exemption to the schedule is requested and granted.

Technical Rationale

Here is the technical rationale for the application of these acceptance criteria to the areas of review addressed by this SRP section:

1. Independent of the regulations of 10 CFR Part 50 or 10 CFR Part 52 that establishes requirements for licensing processes and approaches, the regulatory basis for the staff's technical review for physical security for a nuclear power reactor is established by the requirements of 10 CFR Part 73. Therefore, the staff guidance described in this SRP applies to a license application for or an amendment to an operating license under 10 CFR Part 50 or a combined license under 10 CFR Part 52.

2. Section 10 CFR 52.79(a)(35)(i) and (ii) and 10 CFR 52.79(a)(36)(i) through (v) require that an combined license applicant (or a licensee) must meet all applicable requirements in 10 CFR Part 73 for a physical security plan, safeguards contingency plan, training and qualification plan and cybersecurity plan. The requirements for 10 CFR Part 26, "Fitness for Duty Programs," are in 10 CFR 52.79(a)(44). Under 10 CFR 52.79(a)(35) and

52.79(a)(36), which incorporate by reference 10 CFR Part 73, COL applicants are required to prepare plans that describe a physical protection system (engineered and administrative controls) and a physical protection program that will be constructed, installed, and implemented to protect their facilities against acts of radiological sabotage. After issuance of a COL, the COL holder or licensee is required to implement and maintain the licensing bases (capturing engineered and administrative controls, management systems, and organizations required to operate a nuclear power plant) and meet all applicable regulatory requirements.

3. 10 CFR Part 50 establishes the procedures and criteria for issuing construction permits and licenses to production and utilization facilities. Requirements in 10 CFR 50.33 and 10 CFR 50.34 establish requirements for the FSAR and physical security plans, safeguards contingency plan, and protection against unauthorized disclosure (10 CFR 50.34(c)(1) through 10 CFR 50.34 (c)(3), 10 CFR 50.34(d), and 10 CFR 50.34(e)) that are included in each application for an OL. Licensees must implement physical security requirements as described in the security plan (i.e., licensing bases for security).

4. The acceptable level of detail for the design descriptions of engineered controls (i.e., physical security systems) submitted with a COL application conforms to guidance in RG 1.206. Figure 1 of RG 1.206, "Combined License Application Referencing a Certified Design," illustrates and provides guidance for a minimum for the design scope and design completion for a DC and a COL. The acceptable descriptions of designs and specifications of physical security systems in submitted COL applications is a minimum of 30 percent of a final or 100 percent of a detailed design to provide a reasonable assurance for completion of the detailed designs for procurement, construction, and installations of physical security systems that will meet regulatory requirements of 10 CFR Part 73. Applying a similar framework for review of designs of physical security systems in this SRP section for technical reviews of details of descriptions of licensing bases (capturing required administrative controls, management systems, and organization for how regulatory requirements will be met) ensures uniform technical reviews of the process for meeting standards and criteria for the regulatory findings.

5. Specific to 10 CFR Part 52, the DC review is limited to the designs of physical security systems. The COL applicant citing a DC must provide remaining design descriptions to complete the designs of required physical protection systems, along with the operational requirements and management systems, for meeting all applicable requirements in 10 CFR Part 73. The review of operational requirements and elements of physical protection programs (i.e., administrative controls and management systems) that are relied on or applied physical security systems for establishing physical protection for nuclear material and nuclear operations of an operating reactor are reserved for a COL licensing review. The procurement, construction, and installations of selected physical security systems are verified through required ITA for the determination of 10 CFR 52.103(g) findings.

6. For an OL, the acceptable level of detail is a nearly complete final design requirements and specification (e.g., final designs of systems and required systems interfaces, including the specific information about equipment procured, including manufacturing

data sheets, shop drawings, etc.), and associated design bases for physical security systems. The licensing process under 10 CFR Part 50 is distinct from that established under 10 CFR Part 52 because the regulatory requirements for issuance of an OL require the verification of final design, construction, and installation of physical security systems, along with completion of implementation requirements for administrative controls, management systems, and organizations (e.g., detailed program, policies, processes, procedures, organization, etc.) before the issuance of a license. The details of engineered and administrative controls, management systems, and organization are made available, reviewed, and inspected before determination of Commission findings regarding a request for an OL or amendment to a license.

7. OLs and COLs are similar in standards and criteria under 10 CFR Part 50 and 10 CFR Part 52, with the exception of requirements for ITAAC and 10 CFR 52.103(g) findings that pertain to COLs. The Commission is required to determine whether an application for an operating license meets the standard and requirements of the Atomic Energy Act of 1954 (as amended) and the Commission's regulations, and that notifications (if any) to other agencies and bodies have been duly made, prior to the issuance of operating license or construction permit in accordance with 10 CFR 50.50, "Issuance of Licenses and Construction Permits," and 10 CFR 50.56, "Conversion of Construction Permit to License; or Amendment of License." For an operating license application under part 50 referencing a construction permit that referenced a certified design, the design control document of the selected design addresses, in part, the designs of physical security systems. . The specific conditions under which the Commission may issue an operating license are established in 10 CFR 50.57, "Issuance of Operating License," and 10 CFR 52.97, "Issuances of combined licenses."

8. 10 CFR Part 73, specifies the requirements for designs of physical security systems relied on or credited to implement a physical protection program, by OLs and COLs, including operational requirements and management systems, that protects against internal and external threats up to and including the DBT of radiological sabotage at all times. Compliance with the performance and prescriptive requirements of 10 CFR Part 73, as described above in this section, is required for issuance of a COL or an OL for a nuclear power reactor under 10 CFR Part 52 or 10 CFR Part 50 respectively.

9. The requirements of 10 CFR 52.97, "Issuance of Combined Licenses," requires that the Commission may issue a COL if it finds that: the applicable standards and requirements of the Act and the Commission's regulations have been met; there is reasonable assurance that the facility will be constructed and will operate in conformity with the license, the provisions of the Act, and the Commission's regulations; and issuance of the license will not be inimical to the common defense and security or to the health and safety of the public. The acceptability of the physical security will be based on descriptions that demonstrate (i.e., provide evidence of) how the applicant's proposed engineered and administrative controls, management systems, and organization meet the requirements of 10 CFR Part 52 and 10 CFR Part 73. The requirements in 10 CFR 50.57 set forth the same standards and criteria for the issuance of an OL.

III. REVIEW PROCEDURES

The following factors are in the staff's generic review:

1. The staff bases its review on the identified SRP acceptance criteria stated in Section II of this SRP. The SRP is not a substitute for the NRC's regulations, and compliance with it is not required. Identifying the differences between this SRP section and the design features, analytical techniques, and procedural measures proposed for the facility, and discussing how any proposed alternative measures provide an acceptable method of complying with the regulations that underlie the acceptance criteria, is sufficient to meet applicable requirements for licensing under 10 CFR Parts 50 and 52. For deviations from these acceptance criteria, the staff must review the applicant's evaluation of how the proposed alternatives provide an acceptable method for complying with the relevant NRC requirements identified in Section II of this SRP.

2. The primary reviewer's evaluation of the application for an operating license (i.e., the entire COL or OL application) includes evaluation of the cited technical reports related to the licensing and design bases, as well as of the descriptions of the physical security systems, operational requirements, and management systems. Through this evaluation, the primary reviewer must determine whether the licensing and design bases described by the applicant conform to, and sufficiently address, the design descriptions and requirements identified in SRP Section 13.6.2 for physical security systems, including operational requirements, management systems, and organization. This section provides the basis for acceptance of the application for further technical review. The failure to provide, in the contents of the application, the design descriptions addressing the physical security systems, operational requirements, management systems, and organization conforming to SRP Section II is justification and technical basis for not proceeding with further technical review of a COL or OL application.

3. The reviewer should evaluate only information that has been submitted by the applicant or licensee on the docket. SRP Section 13.6.2 applies to physical review of the designs of the security systems that are located within the nuclear island and structures, PA, and OCA or that relate to the specific structural characteristics, performance, and designs of those structures (e.g., minimum standoff distance).

4. The review of design descriptions includes drawings (plan and section views), line and block diagrams, system and component schematics, system locations and configurations, performance specifications for material and structural construction, specifications for performance, and intended security functions. These descriptions must be at a level of detail sufficient to determine whether the SRP acceptance criteria are met. For a COL application, at a minimum, the level of detail for designs should conform to the guidance provided in RG 1.206, in order to provide reasonable assurance and adequate information for completing detailed designs of physical security systems. For an OL application, a complete final detailed design and descriptions of specific construction and installation standards/criteria (including information about specific vendor equipment, data sheets, and shop drawings for PSS) are reviewed.

5. The focus of the reviewer when evaluating a description of physical security systems and operational requirements for a physical protection program's design must be on the capability of that program to protect against the DBT for radiological sabotage. This evaluation must include how it addresses DID by means of diversity, redundancy, and separation. Where applicable, the system design margins must be reviewed and captured as a part of the design and licensing bases to include procurement, construction, installation, and implementation of operational requirements.

6. For physical security systems and operational requirements associated with the capability for detection, assessment, and response, the review includes how the design of physical security systems addresses DID by means of diversity, redundancy, and separation. Where applicable, the system design margins, as previously discussed, for proposed designs of physical security systems are reviewed and captured as a part of the design basis for detailed designs, procurement, construction, and installation.

7. The acceptance criteria described in this SRP, along with review procedures, apply to both applications and for amendments to existing licenses that are submitted in accordance with the requirements of 10 CFR 50.4, "Written Communications," and 50.90, "Application for Amendment of License, Construction Permit, or Early Site Permit." The acceptance criteria and guidance described in this SRP also apply to the review of alternative measures that are submitted to the NRC in accordance with 10 CFR 73.55(r). Licensees and applicants requesting alternative measures must describe how the proposed alternative measures provide an equivalent and acceptable method of meeting the underlying bases of the relevant NRC requirement which the alternative measure would replace. Additionally, the acceptance criteria described in this SRP apply to the review of security-plan changes that are made by a licensee without prior NRC approval, under 10 CFR 50.54(p)(2).

8. Where an applicant or licensee has submitted a physical security plan that conforms to the most recent NRC-endorsed revision of the generic security plan template, NEI 03-12, for review, the reviewer should confirm that the submitted plan conforms to the format and content of NEI 03-12 and, where applicable, that the generic standard language of the plan sufficiently describes the applicant's licensing bases for how the regulatory requirements that are addressed by the generic text will be met. After confirming that the generic text is appropriate, the reviewer must focus the review on site-specific information. Site-specific information must be sufficiently detailed to describe how all Commission requirements that are associated with the site-specific information will be met. Conformance with NEI 03-12 without sufficient detail for the licensing bases, including site-specific detailed designs of physical protection systems and descriptions that establish the methods to be used to meet the requirements of 10 CFR 73.55 addressed in Section I and Section II above, will not be acceptable for meeting the requirements for an application for an operating license or an amendment to a license. The licensee should describe in the security plan how a deviation from an NRC requirement provides an acceptable method of satisfying the relevant NRC requirements in a way consistent with the acceptance criteria identified in this section of the SRP and in Section II of the SRP above. As described in 10 CFR 73.55(r), alternative measures must be submitted to the NRC in accordance with 10 CFR 50.4 and 10 CFR 50.90.

A. The reviewer should compare the applicant's or licensee's proposed security plan against NEI 03-12 to verify that the template's generic text was followed and that appropriate additional details are provided to describe how regulatory requirements will be met and to establish its licensing bases for physical security. All *{bracketed}* information is reviewed to ensure that descriptions of specific details needed for meeting regulatory requirements have been appropriately addressed.

B. The reviewer should identify any departure from the template text to determine the acceptability of the deviation, to document the technical basis for its acceptability or nonacceptability for meeting regulatory requirements, and to verify that it conforms to these SRP acceptance criteria.

C. The *{bracketed}* text identified in NEI 03-12 is intended to act as a placeholder for each applicant to address and provide additional details of specific proposed physical protection measures, to account for site-specific conditions and to ensure understanding of how the licensee intends to meet certain Commission requirements.

D. The review includes confirming that all *{bracketed}* text is consistent with and complementary to the generic template text in establishing the licensing bases for meeting performance and prescriptive regulatory requirements. Contradictions or inconsistencies between *{bracketed}* text and generic template text, or within the security plan (i.e., between the PSP, T&QP, and SCP), should be identified and resolved by the applicant or licensee to clearly establish the bases for licensing.

The Staff's Specific Physical Security Review

The staff will review the applicant's licensing bases related to a requested licensing action and confirm whether they are acceptable if the applicant provides sufficient data and information in the docketed license application (e.g., security plans, FSAR, and other licensing-basis documents) to meet each of the following requirements:

1. 10 CFR 73.1, "Purpose and Scope"

A. Review of the descriptions of how a design and implementation of a physical protection system address the capabilities of protecting the nuclear power plant against acts of radiological sabotage and preventing theft or diversion of special nuclear material.

B. Review of the descriptions of potential radiological sabotage analyzed under 10 CFR 73.55 and their postulated credible bounding scenarios to confirm that they meet the criteria set forth in 10 CFR 73.1(a)(1) for protection against radiological sabotage and that the detailed descriptions in the Security Plan that describe or specify this radiological sabotage conform to guidance on characteristics of the DBT adversary and capabilities specified in RG 5.69.

C. Review confirms that RG 5.69 is incorporated in whole and that this is explicitly stated in the descriptions contained in security plan. NRC guidance for inspections and guidance developed by industry for inspections are not Commission determined regulatory requirements for characteristics of the DBT and are not acceptance criteria for licensing.

D. The requirements of 10 CFR 73.1(a)(2) through 73.1(a)(9) are not within the scope of review. Reviewers evaluate whether the proposed descriptions of radiological sabotage conform to appropriate guidance for assessing radiological sabotage in RG 5.69, RG 5.76, and RG 5.81.

2. 10 CFR 73.2, "Definitions"

A. Reviewers evaluate whether the descriptions and application or use of terms in the security plans are as stated in the definitions in 10 CFR 73.2 and conform to guidance provided in regulatory guides (e.g., RG 5.69, RG 5.74, RG 5.76, RG 5.77, RG 5.81 etc.).

B. In accordance with the requirements of 10 CFR 73.3, "Interpretations," terms are identified and checked against their corresponding definitions; their meaning is established by the written interpretation of the NRC's General Counsel to be binding upon the Commission. Reviewers should consult with OGC about acceptability when a different term (as a matter of preference) is provided in descriptions of the licensing bases but has the same meaning and/or functions described in the official definition of another term.

3. 10 CFR 73.3, "Interpretations"

Where required, the staff requests that OGC provide written interpretations of definitions and regulations as stated in 10 CFR Part 73. The NRC security technical reviewers make determinations only about the technical aspects of meeting regulatory requirements.

4. 10 CFR 73.4, "Communications"

Applicants and licensees submit information and reports to the licensing docket in accordance with requirements of 10 CFR Part 50 or 10 CFR Part 52.

5. 10 CFR 73.5, "Specific Exemption"

A request for a specific exemption can be included in Part 1 of the COLA or OL application. The standards and criteria set forth in the licensing regulations of 10 CFR 50 or 10 CFR 52 are applied in the review and consideration of such requests.

6. 10 CFR 73.8, “Information Collection Requirements: OMB Approval,” and 10 CFR 73.20, “General Performance Objective and Requirements”

   These sections are not applicable to or within the scope of technical review.

7. 10 CFR 73.21, “Protection of Safeguards Information: Performance Requirements” and 10 CFR 73.22, “Protection of Safeguards Information: Specific Requirements”

   A. The review of the descriptions of information and dates in the license application verifies that the application describes how a management system (i.e., program, process and procedures), operational requirements, and organization will be established to implement the protection of SGI in accordance with the requirements set forth in 10 CFR 73.21 and 10 CFR 73.22.

   B. The descriptions for managing SGI, established in implementing procedures, should include standards and criteria for controls necessary to: (1) protect SGI from unauthorized disclosure, (2) prepare, identify, handle, and store SGI, (3) protection in, (4) implement internal and external controls for transit and correspondence, (5) perform inspections, audits, and evaluation of the SGI program and its implementation, (6) establish conditions for access to SGI, including application of a “need to know,” (7) control reproduction and dissemination of SGI, (8) meet requirements for protecting SGI on electronic systems, (9) remove the SGI designation, and (10) destroy SGI.

   C. If the applicant’s or licensee’s plans to protect SGI are in accordance with protection procedures employed by the NRC, they are acceptable as methods of protection against unauthorized disclosure.

8. 10 CFR 73.23, “Protection of Safeguards Information—Modified Handling: Specific Requirements” is not applicable to or within the scope of review for a nuclear power reactor license in accordance with requirements of 10 CFR Part 50 or 10 CFR Part 52.

9. The following regulatory requirements are not within the scope of review for an application to operating a nuclear reactor pursuant to the requirements of 10 CFR Part 50 or 10 CFR Part 52:

   A. 10 CFR 73.24, “Prohibitions”

   B. 10 CFR 73.25, “Performance Capabilities for Physical Protection of Strategic Special Nuclear Material in Transit”

   C. 10 CFR 73.26, “Transportation Physical Protection Systems, Subsystems, Components, and Procedures”

   D. 10 CFR 73.27, “Notification Requirements”

   E. 10 CFR 73.28, “Security Background Checks for Secure Transfer of Nuclear Materials”

F. 10 CFR 73.35, “Requirements for Physical Protection of Irradiated Reactor Fuel (100 Grams or Less) in Transit”

G. 10 CFR 73.37, “Requirements for Physical Protection of Irradiated Reactor Fuel in Transit”

H. 10 CFR 73.45, “Performance Capabilities for Fixed Site Physical Protection Systems.”

I. 10 CFR 73.46, “Fixed Site Physical Protection Systems, Subsystems, Components, and Procedures”

J. 10 CFR 73.50, “Requirements for Physical Protection of Licensed Activities”

K. 10 CFR 73.51, “Requirements for the Physical Protection of Stored Spent Nuclear Fuel and High-Level Radioactive Waste”

10. 10 CFR 73.40, “Physical Protection: General Requirements at Fixed Sites”

A. A licensee shall provide physical protection at a fixed site or contiguous sites where licensed activities are conducted, against radiological sabotage, or against theft of special nuclear material, or against both, in accordance with the applicable sections of 10 CFR Part 73 for each specific class of facility or material license.

B. The licensee shall establish and maintain physical security in accordance with security plans approved by the NRC.

11. 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”

The applicant describes how the requirements of 10 CFR 73.54 will be met in a cyber-security plan. The staff review of the adequacy of how an applicant or licensee plans to meet these regulatory requirements is established in SRP 13.6.6 and is outside the scope of this SRP Section.

Physical Security Plan

1. 10 CFR 73.55(a), “Introduction”

Security plans must identify, describe, and account for site-specific conditions that affect the licensee’s capability to satisfy the requirements of 10 CFR 73.55.

Licensees are responsible for maintaining the onsite physical protection program in accordance with Commission regulations through the implementation of security plans and written security-implementing procedures.

Applicants for an operating license under the provisions of 10 CFR Part 50 or holders of a COL under the provisions of 10 CFR Part 52 shall implement the requirements of 10 CFR 73.55 before fuel is allowed on site inside the protected area as described in 10 CFR 73.55(a)(4). Regulatory Guide (RG) 5.76, "Physical Protection Programs at Nuclear Power Reactors," contains additional guidance concerning this requirement.

Applicants for an operating license under the provisions of 10 CFR Part 50 or holders of a COL under the provisions of 10 CFR Part 52 that do not cite a standard DC or that cite a standard DC issued after May 26, 2009, shall meet the requirement of 10 CFR 73.55(i)(4)(iii) to locate the secondary alarm station (SAS) inside the protected area and configure the SAS to the same standards and for the same capabilities as the central alarm station (CAS).

Guidelines

Implementing procedures are not required to be submitted as part of the security plan; however, should the staff reviewer determine that additional information that would otherwise be contained in an implementing procedure is needed to understand how a security plan's requirement satisfies a Commission requirement, the reviewer should request that such information be provided and the information gained from the licensee should be documented in the reviewer's final evaluation report as part of the security-plan review process.

The staff reviews the description of the physical security program in Section 13.6 of the FSAR. The NRC staff reviews the FSAR's description of the physical security program in Section 13.6 (which should include Table 13.4-201, "Operational Programs Required By NRC Regulations") to ensure that implementation milestones are associated with these programs:

- physical security program
- training and qualification program
- safeguards contingency program
- FFD program for security
- personnel fitness for duty (FFD) program for construction (workers and first-line supervisors)
- physical protection program (applicable to protection of special nuclear material before to the protected area is declared operational)
- FFD program for construction (management and oversight personnel)
- FFD program for FFD program personnel

- cyber security program

Additional guidance is provided in RG 5.76.

2. 10 CFR 73.55(b), “General Performance Objectives and Requirements”

The licensee shall establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high 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 physical protection program must protect against the DBT of radiological sabotage as stated in 10 CFR 73.1.

The physical protection program must be designed to prevent significant core damage and spent fuel sabotage. Specifically, the program must:

- ensure that the ability to detect, assess, interdict, and neutralize threats, up to and including the DBT of radiological sabotage, as stated in 10 CFR 73.1, is maintained at all times

- provide DID through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures, as needed, to ensure the effectiveness of the physical protection program

The licensee shall analyze and identify site-specific conditions, including target sets, that may affect the specific measures needed to implement the requirements of 10 CFR 73.55 and shall account for these conditions in the design of the physical protection program.

Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability to meet Commission requirements through the implementation of the physical protection program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures.

The licensee shall establish, maintain, and implement a performance evaluation program, in accordance with Section VI of Appendix B to 10 CFR Part 73, to demonstrate and assess the effectiveness of the physical protection program that includes the capability of armed responders and armed security officers to implement the licensee’s protective strategy.

The licensee shall establish, maintain, and implement an access-authorization program in accordance with 10 CFR 73.56 and shall describe the program in the physical security

plan. This description may be provided through a requirement in the security plan that the licensee will follow the guidance provided in RG 5.66 for:

- applicability
- general performance objectives
- backgrounds investigation
- psychological assessment
- behavioral observation
- self-reporting of legal actions
- granting unescorted access and certifying unescorted access authorization

The licensee shall establish, maintain, and implement a cyber-security program in accordance with 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." The licensee is required to address the CSP as part of the physical protection program; however, the review of the CSP is not addressed in this SRP. The CSP is addressed in SRP 13.6.6, "Cyber Security Plan."

The licensee shall establish, maintain, and implement an Insider Mitigation Program (IMP) and shall describe the program in the physical security plan in accordance with 10 CFR 73.55(b)(9)(i) and (ii).

The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining authorization for unescorted access to a protected or vital area and implement DID methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's ability to prevent significant core damage and spent fuel sabotage.

The insider mitigation program must contain elements from:

- the access-authorization program described in 10 CFR 73.56
- the FFD program described in 10 CFR Part 26
- the cyber security program described in 10 CFR 73.54
- the physical protection program described in 10 CFR 73.55

The licensee shall use the site's corrective-action program to track, trend, correct, and prevent the recurrence of failures and deficiencies in the physical protection program.

The licensee must coordinate the implementation of security plans and associated procedures with other onsite plans and procedures to preclude conflict under both normal and emergency conditions.

Guidelines

The physical security plan shall describe the programs, systems, and measures that the licensee implements to support the overall physical protection of the site and confirm that they meet the general performance objective and requirements of 10 CFR 73.55.

The licensee shall design and maintain the physical protection program to prevent significant core damage and spent fuel sabotage as well as to ensure the protection of special nuclear material possessed by the licensee as described in their NRC-issued license or as otherwise authorized by the NRC.

Key physical protection system elements should include security personnel, detection and assessment systems, physical security barriers, access controls, search programs, cyber security, information security, personnel security, and contingency plans.

The physical security plan shall fully describe the access-authorization program, in accordance with 10 CFR 73.56, although a full description is not necessary when the plan confirms that the licensee has used the most current revision of RG 5.66, "Access Authorization Program for Nuclear Power Plants." RG 5.66 provides acceptable language for insertion into site security plans to describe the access-authorization program.

The physical security plan fully describes the insider mitigation program, in accordance with 10 CFR 73.55 (b)(9)(i) and (ii) and 10 CFR 73.56, although a full description is not necessary when the plan confirms that the licensee has used the most current revision of RG 5.77, "Insider Mitigation Program." RG 5.77 provides guidance for an IMP that would meet the requirements in 10 CFR 73.55(b)(7) and (b)(9) and the latest NRC-staff-endorsed version of the industry's guidance document, Nuclear Energy Institute (NEI) 03-01, "Nuclear Power Plant Access Authorization Program." These sources provide an acceptable approach for an IMP that meets the provisions of 10 CFR 73.55 as part of the licensee's physical security plan.

3. 10 CFR 73.55(c), "Security Plans"

Guidelines

A. Licensee security plans:

The physical security plan shall describe how the licensee will implement requirements of 10 CFR 73.55 through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, the implementation of predetermined response plans and strategies, and the protection of digital computer and communication systems and networks.

The physical security plan shall describe any site-specific conditions that affect how the licensee implements Commission requirements.

B. The physical security plan shall describe protection of security plans. The licensee shall protect the security plans and other security-related information against unauthorized disclosure in accordance with the requirements of 10 CFR 73.21.

C. Physical security plan. The licensee shall establish, maintain, and implement a physical security plan that describes how the performance objective and requirements set forth in 10 CFR 73.55 will be implemented.

D. Training and qualification plan. The licensee shall establish, maintain, implement, and follow a T&QP that describes how the criteria set forth in Section VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," of Appendix B to 10 CFR 73 will be implemented.

E. Safeguards contingency plan. The licensee shall establish, maintain, and implement an SCP that describes how the criteria set forth in Section II, "Nuclear Power Plant Safeguards Contingency Plans," of Appendix C to 10 CFR 73 will be implemented.

F. Cyber security plan. The licensee shall establish, maintain, and implement a CSP that describes how the criteria set forth in 10 CFR 73.54, ''Protection of Digital Computer and Communication Systems and Networks,'' will be implemented.

The physical security plan shall describe security implementing procedures as described in 10 CFR 73.55(c)(7).

(i) The licensee shall have a management system to provide for the development, implementation, revision, and oversight of security procedures that implement Commission requirements and the security plans.

(ii) Implementing procedures must document the structure of the security organization and detail the types of duties, responsibilities, actions, and decisions to be performed or made by the person in each position of the security organization.

(iii) The licensee shall:

a) provide a process for the written approval of implementing procedures and revisions by the individual with overall responsibility for the security program

b) ensure that revisions to security implementing procedures satisfy the requirements of 10 CFR 73.55

(iv) Implementing procedures need not be submitted to the Commission for approval, but are subject to inspection by the Commission.

The requirement in 10 CFR 73.55(c)(1)(ii) is that "Licensee security plans must describe site-specific conditions that affect how the Licensee implements the requirements."

4. 10 CFR 73.55(d), “Security Organization”

The physical security plan describes how the security organization will meet the following:

A. Establish an organization structure and required management system (i.e., policy, process, procedures, etc.) that will oversee the site’s physical protection program. The descriptions should address the purpose, goals, objectives, functions, and the role of the security organization within the plant organization and management structure for conducting operations. The plant’s organizational structure provides assurance of independence between the management of the security organization and the management of power production to avoid potential conflicts of organizational goals and responsibilities.

B. Establish a security organization will operate within the defined processes, including the use of procedures, to conduct the operations in Chapter 13 of the FSAR. Where descriptions of the management system in the FSAR are relied on to describe how a management system will be provided, the PSP explicitly incorporate by reference the FSAR chapter and information. The descriptions indicate that procedures are a means of implementing security requirements and conducting security operations.

C. Establish management systems that include processes and procedures to develop, revise, implement, and review security programs, including change control and the safety/security interface. Identify individuals within and outside the security organization with duties and responsibilities for review and approval for assurance that review and management of the safety/security interface comply with the requirements of 10 CFR 73.58.

D. Establish the minimum staffing, authority, availability, and assigned duties of members of the security organization, including their authority and availability to meet all of the prescriptive regulatory requirements. The descriptions should include the position titles, the roles and responsibilities, and the authority allotted in directing day-to-day and contingency operations. Specify duties and responsibilities for the command and control of the security force. Identify that the assigned individual is available onsite within the PA, is available and reliable to perform duties and responsibilities at all times, and individuals are not assigned duties and responsibilities that would interfere with directing normal day-to-day and contingency security operations. Include the minimum staffing for this security organization in the list of the minimum staff in FSAR Chapter 13, but identify the required minimum staffing for armed response and protected as SGI which is protected and withheld from disclosure, and therefore is not shown in the plant’s minimum staffing.

E. Descriptions of the management system must indicate that any individual will be prohibited from implementing 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 T&QP provided to meet the requirements of Section VI of Appendix B to 10 CFR Part 73.

F. Descriptions of the assigned duties of non-security personnel. The descriptions in the T&QP may be incorporated by reference, provided that the specific information is cited or stated that these personnel must: (1) be trained, qualified, and periodically requalified to perform their assigned duties; (2) be properly equipped to perform assigned duties; (3) have the knowledge, skills, and abilities, including physical attributes such as adequate sight and hearing for individuals assigned security duties and responsibilities.

G. Descriptions of other positions in the security organization, which should include but are not limited to: (1) security manager; (2) access-authorization supervisor or access-authorization/FFD supervisor; (3) security shift supervisor; (4) armed-responder team leader; (5) armed responders; (6) armed security officers; (7) alarm-station operators; (8) watchpersons, and (9) security instructors.

Guidelines

The physical security plan shall describe the security organization. An acceptable physical security plan would identify the positions within the security organization by position title, with a position description for each. The security plan shall, at a minimum, include these generic position titles and a position description for each: security manager, access authorization supervisor or access authorization or FFD supervisor, security shift supervisor, armed-response team leader, armed responders, armed security officers, alarm station operators, watchpersons, and security instructors. The security plan shall also meet the requirements described in 10 CFR 73.57 for performing criminal history checks of individuals granted unescorted access to a nuclear power facility or SGI. Terms such as “manager,” “supervisor,” and “chief” are often used interchangeably in common speech and in most cases do not change the position descriptions, duties, or responsibilities of personnel filling the position. However, reviewers should pay close attention to how the licensee uses these terms within their security plan and should ensure that the licensee uses these titles and position descriptions consistently throughout the security plan and its appendices. It is especially important that position titles be consistent between the Critical Task Matrix described in Appendix B of the security plan and the roles and responsibilities described in Appendix C of the security plan. The position descriptions should remain consistent between the PSP, T&QP, and SCP.

An acceptable physical security plan shall confirm that the licensee will not assign any duties or responsibilities to personnel within the security organization that would conflict with those duties and responsibilities required for protection against radiological sabotage.

The physical security plan shall confirm that the security organization is designed, staffed, trained, qualified, and equipped to implement the physical protection program, including the protective strategy.

An acceptable physical security plan would identify, by position titles and descriptions, the management system that provides oversight of the onsite physical protection program, and would specify by position title and description the individual responsible to develop, revise, implement, and oversee security procedures.

The physical security plan should describe how written approvals of procedures and revisions by the individual with overall responsibility for the site security program (security director or manager) are a part of the management system.

The physical security plan should describe, by position title and description, the individual who is onsite at all times who has the authority to direct the activities of the security organization. This individual should not be assigned any other duties that would interfere with his or her ability to perform the security organization's assigned duties.

An acceptable physical security plan would describe the use of both members of the security organization and non-security-organization personnel (such as warehouse personnel performing package searches) who are assigned duties and responsibilities required to implement the physical protection program. The security plan should confirm that all individuals who are assigned any duties and responsibilities required to implement any part of the physical protection program are properly equipped to perform those assigned duties and responsibilities and that they possess the knowledge, skills, and abilities, including physical attributes (adequate sight and hearing), to perform their assigned duties and responsibilities.

When contractors are used, an acceptable physical security plan should describe how contracted individuals are incorporated into the physical protection program, including the protective strategy, and would confirm that these individuals are trained and qualified to perform the functions that they are assigned within the security organization. An acceptable physical security plan would state that the contract is retained as a record.

An acceptable physical security plan would confirm that at least one member of the security organization is onsite and available at all times and has the authority to direct the activities of the security organization and is not assigned any other duties that would interfere with his or her ability to perform these duties in accordance with the security plans and the licensee's protective strategy.

An acceptable physical security plan would confirm that the licensee will 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 Section VI of Appendix B to 10 CFR 73 and the Training and Qualification Plan. Non-security personnel may be assigned duties and responsibilities required to implement the physical protection program and shall:

A. be trained through established licensee training programs to ensure that each individual is trained, qualified, and periodically requalified to perform such assigned duties

B. be properly equipped to perform such assigned duties

C. possess the knowledge, skills, and abilities, including physical attributes such as adequate sight and hearing, required to perform such assigned duties and responsibilities

5. 10 CFR 73.55(e), “Physical Barriers”

Guidelines

An acceptable physical security plan would confirm that access to the protected area is controlled through physical barriers. The physical security plan would also describe the general location; construction standards; and specific function to be performed by each physical barrier used in the OCA, protected area, and vital areas.

An acceptable physical security plan shall confirm that the reactor control room, the central alarm station, and the location within which the last access-control function for access to the protected area is performed are bullet-resisting. For COL applicants, this would include the secondary alarm station, in accordance with 10 CFR 73.55(i)(4)(iii).

An acceptable physical security plan shall describe the bullet-resisting physical barriers used for the reactor control room; central alarm station; bullet-resisting protected positions; the location within which the last access control function for access to the protected area is performed; and, for COL applicants, the secondary alarm station, in accordance with 10 CFR 73.55(i)(4)(iii). An acceptable physical security plan would typically define “bullet-resisting” or “bullet resistant” as having a minimum capability of resisting a high-powered rifle round, as identified in RG 5.76 “Physical Protection Programs at Nuclear Power Reactors.”

An acceptable physical security plan will describe the use of all physical barriers (to include natural terrain) used in the OCA, protected area, and vital areas to implement the site’s physical protection program. This description should include the type of barriers used, a general description of the construction of each barrier, (e.g., buildings, topography, fences, walls, doors, etc.) and the specific function to be performed by each barrier used.

Additional guidance is provided in RG 5.76, “Physical Protection Programs at Nuclear Power Reactors.”

6. 10 CFR 73.55(e)(7), “Isolation Zones”

Guidelines

An acceptable physical security plan shall describe the location of isolation zones and areas of the protected area’s perimeter where isolation zones are not maintained because of site-specific characteristics, as identified in 10 CFR 73.55(e)(8)(iv).

This description shall confirm the use of intrusion-detection equipment within each isolation zone and shall confirm that the intrusion-detection equipment used is capable

of detecting attempted and actual penetration of the protected area's perimeter barrier before such penetration can be completed. Additionally, this description shall also confirm that isolation zones are monitored with assessment equipment capable of providing real-time recording and playback of video images of detected activities before and after each alarm annunciation.

7. 10 CFR 73.55(e)(8), "Protected Area"

Guidelines

An acceptable physical security plan shall describe protected-area barriers that are consistent with the definitions provided in 10 CFR 73.2.

This description should address the extent to which the protected-area barrier is separated from vital-area barriers, areas where building walls or roofs comprise a portion of the protected area's perimeter barrier and areas where isolation zones are not maintained. This description should specify the types of barriers that are used and the intrusion-detection and -assessment capabilities that are in place to protect these areas, including the function of each to meet the requirements of 10 CFR 73.55.

An acceptable physical security plan shall describe the protection provided against penetrations of the protected-area barrier, including unattended openings that intersect a security boundary, such as underground pathways. This description shall confirm that unattended openings and underground pathways are protected, as required by 10 CFR 73.55(e)(8)(ii) and 10 CFR 73.55(i)(5)(iii).

8. 10 CFR 73.55(e)(9), "Vital Areas"

Guidelines

An acceptable physical security plan shall confirm that areas containing vital equipment are identified and protected as vital areas.

The physical security plan shall confirm that access to vital equipment requires passage through at least two physical barriers, that each barrier meets the definition for physical barriers in 10 CFR 73.2, that all points of personnel and vehicle access into a vital area are positively controlled, and that these points of personnel and vehicle access are locked and alarmed.

An acceptable physical security plan shall describe the areas in which vital equipment has been identified and would provide a list of those areas that the licensee has designated as vital areas. At a minimum, vital areas must include the reactor control room; the spent fuel pool; the central alarm station; and, for COL applicants, the secondary alarm station, in accordance with 10 CFR 73.55(i)(4)(iii).

An acceptable physical security plan shall describe where the secondary power-supply system for alarm-annunciation equipment and the secondary power-supply system for non-portable communication equipment are located within the vital area.

9. 10 CFR 73.55(e)(10), “Vehicle Control Measures” (Vehicle Barriers)

Guidelines

An acceptable physical security plan shall describe the use, placement, and function of vehicle-control measures in the OCA, PA, and VAs if applicable. The licensee shall provide legible site-specific drawings or maps that clearly identify all land-based and water-based vehicle barrier systems used, including active and passive barriers.

The description should provide detailed information regarding the facility’s use of vehicle barriers to meet the requirements of 10 CFR 73.55 for protection against the DBT vehicle bomb, as described in 10 CFR 73.1. RG 5.69 “Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements” contains additional details about the characteristics of the design-basis vehicle threat.

The physical security plan shall confirm that periodic checks for the operability of active vehicle barrier systems are performed and that the specific procedures for each check are contained in facility procedures.

The physical security plan shall describe the types of periodic surveillance and observation of land- and water-based vehicle barrier systems (e.g., using alarms, cameras, patrols, etc.) to detect indications of tampering and degradation and to ensure that the systems can perform their intended functions.

The physical security plan shall describe the protective measures for rail access to the protected area and confirm that a train derailer is installed, or that a section of track has been removed, or that access to railroad sidings is restricted, and that periodic surveillance of the protective measures is implemented. The physical security plan shall.

The physical security plan shall describe the surveillance methods implemented for the protective measures at rail access points.

Additional guidance is provided in RG 5.69.

10. 10 CFR 73.55(f), “Target Sets”

Guidelines

An acceptable physical security plan shall confirm that the licensee has established and implemented a process for identifying and grouping target sets. The plan should confirm that a process exists for the oversight of target-set equipment and systems that includes handling configuration changes that could change the licensee’s protective strategy. The plan should also confirm that the details of this process are in implementing procedures.

The physical security plan shall describe the process the licensee has established and implemented to develop and identify target sets, including a description of how target sets are identified and grouped. This description should generally identify the types of subject-matter experts who are used to perform the analysis needed and the minimum areas of technical expertise/knowledge that will be represented by the assembled subject-matter experts.

The physical security plan shall confirm that cyber-attacks were considered during the development and identification of target sets and that the specific cyber security measures that are used to provide protection against cyber-attacks are contained in a cyber-security plan required by 10 CFR 73.54. Additional guidance is provided in RG 5.71, "Cyber Security Program for Nuclear Facilities."

The physical security plan shall confirm that the licensee's protective strategy accounts for target-set equipment that is not located within a protected or vital area. The security plan should generally address how such target-set equipment is handled within the response strategy and how this equipment is accounted for in drills and exercise scenarios. The security plan should also explain how changes to target sets, where appropriate, are coordinated between operations and security, documented in ways consistent with the safety/security interface requirements contained in 10 CFR 73.58, and accounted for in changes to the licensee's protective strategy where needed.

The security plan shall confirm that a process exists for the oversight of target-set equipment and systems that includes handling configuration changes that could change the licensee's protective strategy. The security plan should generally describe the process to be used to meet the oversight requirement (i.e., use of patrols, cameras, personnel in bullet resistant enclosures, etc.).

The security plan shall confirm that changes to the configuration of target sets are coordinated between operations and security, and that such changes are documented in ways consistent with safety/security interface requirements contained in 10 CFR 73.58. The security plan shall describe the process that will used to inform security management of such target-set changes, analyze the changes for impact to the response strategy, and ensure that changes to the licensee's protective strategy are communicated to response personnel where needed.

The focus of this review is to confirm that the licensee has established and implemented a process for the identification of target sets. Verification that the methods used and the groupings made by a licensee are technically accurate and complete will be made during inspection activities.

Additional guidance is provided in RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors."

11. 10 CFR 73.55(g), “Access Controls”

Guidelines

The staff reviewer should verify that the physical security plan describes all vehicle, personnel, and material access-control points used at the facility, including the function of each and the measures that are implemented at each access control point to positively identify vehicles, personnel, and materials and limit access to only authorized vehicles, personnel, and materials.

The physical security plan should describe the measures to be implemented at each location to ensure that only authorized personnel, material, and vehicles are granted access beyond these locations. This description should generally address the functions to be performed by the personnel assigned to each location and the functions to be accomplished through the measures implemented at each location.

12. 10 CFR 73.55(g)(1)(i)—Access-Control Points, Badging, and Responsible Personnel

Guidelines

The security plan shall confirm that all access portals are either located outside of, or are collocated with, the physical barrier for which they control access. The security plan should also identify the general location of each access-control point in relation to the physical barrier through which it is used to grant access, as well as the identify the type of area to which it controls access (e.g., owner-controlled area, protected area, or vital area).

The physical security plan shall confirm that access-control portals are equipped with locking devices, intrusion-detection equipment, and surveillance equipment that are consistent with the function to be performed at each access control point. This description should include a general description of the types of locking mechanisms and intrusion-detection systems that are used and how surveillance will be provided. This description should identify the location at which alarm annunciation will be made, the location from which surveillance will be provided, and the personnel who will be monitoring alarm annunciations and surveillance equipment.

The staff reviewer should verify that the physical security plan describes the process used to provide supervision and control over the badging process to prevent unauthorized bypass of the access-control equipment located at or outside the protected area. This description should identify physical barriers that are used and any surveillance equipment used and should confirm that cyber security measures are in place to prevent or detect attempts to manipulate computer systems used as part of the badge process.

The security plan shall confirm that unescorted access to the protected area and vital areas during non-emergency conditions is limited to only those individuals who require unescorted access to perform assigned duties and responsibilities.

An acceptable physical security plan shall confirm that an individual located in a bullet-resisting structure is responsible for the last access control function into the protected area. The security plan should describe the individual's or post's duties to be performed for the purpose of controlling admission to the protected area, and should specify whether this individual provides response capabilities or would only summon assistance during security events. The security plan should specify the response duties of this individual, including any redeployment during a contingency event. The security plan should confirm that access portals are secured before this individual is redeployed.

13. 10 CFR 73.55(g)(1)(ii) —Vehicle-Control Measures

Guidelines

An acceptable physical security plan would adequately describe the location of vehicle barriers used (in the owner-controlled areas, protected area, and vital areas) and the processes to be followed (that are consistent with the intended function to be performed) at each owner to ensure that only authorized vehicles are granted access through the barrier.

The physical security plan should describe how search functions (in the protected area and if applicable OCA) are performed (10 CFR 73.55(h)) and observed to ensure that a response can be initiated in accordance with 10 CFR 73.55(h).

Site maps and diagrams provided by the licensee that are part of the security plan should depict the location of passive components of the vehicle barrier systems and active components at access control points.

14. 10 CFR 73.55(g)(2)—Protected-Area Access

Guidelines

An acceptable physical security plan shall confirm that before granting access into the protected area, a process is in place to identify individuals before granting access beyond the barrier. The security plan shall describe how the licensee will obtain confirmation of an individual's identity through a combination of a photo identification badge possessed by the individual and the use of biometric equipment such as hand-geometry. Confirmation of identity is usually made after the individual has successfully met all search requirements.

The physical security plan shall confirm that that the licensee has established and implemented processes at protected-area access-control portals to verify that individuals, vehicles, and materials are authorized access before granting them entry into the protected area. The security plan shall describe the methods used to verify access authorization. Generally, a determination of access authorization is confirmed by digital programming parameters associated with badges and biometrics.

The physical security plan shall confirm that personnel entering the protected area are not currently denied access to another licensed facility.

The physical security plan shall confirm that all personnel, material, and vehicles are subjected to the search process, as required by 10 CFR 73.55(h), and have met requirements for positive identification and authorization for access before they are permitted to enter the protected area. The reviewer should verify that the description of search activities is sufficiently detailed and that the location at which search functions are performed is specified.

Physical layout diagrams that are part of the security plan should depict the location of the protected-area barrier and the access-control points through the barrier.

15. 10 CFR 73.55(g)(3)—Vehicles in the Protected Area

An acceptable physical security plan would confirm that vehicles in the protected area are operated only by personnel who possess unescorted access privileges and have been authorized to use the vehicle, including confirmation that use of the vehicle is for authorized purposes in support of plant functions or emergency conditions. The physical security plan should require confirmation that keys must be removed from the vehicle or that the vehicle is otherwise disabled when not in use.

The physical security plan should confirm that personnel who do not possess unescorted access privileges and who operate vehicles within the protected area are escorted by an individual who is capable of maintaining continuous communication with both alarm stations, as required by 10 CFR 73.55(g)(8).

The physical security plan shall confirm that vehicles transporting hazardous materials inside the protected area are escorted by an armed member of the security organization who has continuous communication capability with the alarm stations.

16. 10 CFR 73.55(g)(4)—Vital Areas

Guidelines

An acceptable physical security plan shall require confirmation that access to vital areas during nonemergency conditions is limited to individuals who require access to perform their duties in ways consistent with 10 CFR 73.55(g)(1)(i)(D). The physical security plan should also confirm that access to vital areas is controlled in ways consistent with vital-area access-authorization lists.

The physical security plan shall confirm that the licensee has implemented a process to assess the continued need of individuals to access specific vital areas to perform duties and responsibilities. The physical security plan shall confirm that, at a minimum, this process includes the periodic review of access-authorization lists no less frequently than every 31 days as specified in 10 CFR 73.56(j) The physical security plan should confirm that periodic reviews are performed by a cognizant manager or supervisor at the licensee or applicant who is responsible for directing the work activities of the individual who is being granted unescorted access.

The physical security plan shall confirm that the licensee has developed procedures to respond to a site-specific credible threat or other credible information. The physical security plan should confirm that implementing procedures include a two-person (line-of-sight) rule for all personnel in vital areas so that no single individual is permitted unobserved access to a vital area.

17. 10 CFR 73.55(g)(5)—Emergency Conditions

Guidelines

An acceptable physical security plan shall describe ~~confirm that~~ the access-control system is designed to accommodate the need for rapid entry and exit of authorized individuals during emergency conditions or situations.

The physical security plan shall confirm that security-implementing procedures for emergency conditions address the processes to be used to verify the identity of emergency personnel without unnecessarily delaying them to ensure prompt access by authorized emergency personnel to affected areas and equipment.

18. 10 CFR 73.55(g)(6)—Access-Control Devices

Guidelines

An acceptable physical security plan would describe the types of security keys, locks, combinations, passwords, and related access-control devices used at the facility and would describe how the access-control devices that are used to secure and/or access protected areas, vital areas, and security systems are controlled to reduce the probability of compromise. The physical security plan shall confirm that a process is in place to control the issuance of access-control devices and to account for all access-control devices at least annually.

The physical security plan shall confirm that a process is in place, including implementing procedures, to ensure that only those individuals who are authorized to have unescorted access to a protected area, vital area, or security system in performance of their official duties are granted such access or are issued access-control devices such as locks, keys, combinations, and passwords that can be used to secure and/or access those areas or systems.

The physical security plan shall confirm that a process is in place to control the issuance of access-control devices and to account for all access-control devices at least annually. This description should include confirmation that a record (i.e., key control log) is maintained that identifies each access-control device used, to whom that device was issued, and when it was returned. The physical security plan shall also confirm that a process to account for access-control devices at least annually is established.

The physical security plan shall confirm that compensatory measures are implemented when the licensee suspects that access-control devices may have been compromised and implements a process to retrieve, change, rotate, deactivate, or otherwise disable

the affected access-control devices when an individual's access to such areas and devices has been terminated under less-than-favorable conditions. The physical security plan should describe the timeframe in which the licensee will initiate and complete compensatory measures or other required actions for conditions that could degrade the security program.

19. 10 CFR 73.55(g)(6)(ii)—Photo Identification

Guidelines

An acceptable physical security plan shall confirm that a numbered picture-badge identification system is used for all individuals who are authorized to have unescorted access to protected and vital areas. The physical security plan should confirm that a record is maintained that includes the names and affiliation of all individuals to whom a numbered picture badge has been issued and the areas to which unescorted access is granted.

The physical security plan shall describe whether the numbered photo-identification badges are authorized to be removed from the protected area or not. If removal is authorized, the physical security plan should describe the measures that are in place to verify the identity of each individual in possession of a numbered photo-identification badge before granting them access to ensure that their numbered photo identification badge has not been compromised and is not otherwise being used by unauthorized personnel (e.g., badge deactivation on exit or confirmation of identity and authorization before entry).

The physical security plan shall confirm that the numbered photo-identification badges are clearly displayed while individuals are inside the protected area or vital areas and should confirm that implementing procedures provide specific instruction to employees for how the numbered photo-identification badges will be displayed. Generally, employees should be instructed to wear the numbered photo-identification badges on the upper front portion of the body to be clearly visible except when operational safety concerns require otherwise.

The physical security plan shall confirm that a record is maintained that includes the names and affiliation of all individuals to whom photo-identification badges have been issued and the areas to which unescorted access is granted. The physical security plan shall also confirm that a process to account for access-control devices at least annually is established.

20. 10 CFR 73.55(g)(6)(iii)—Personnel in the Access-Authorization Program

The physical security plan shall specify whether access-authorization program personnel are given passwords, combinations, or other access-control devices that can be used to gain access to the protected area or that could be used to gain access to the protected area through manipulation of access-control equipment or systems. The physical security plan shall confirm that such personnel who are given passwords, combinations,

or other access-control devices meet the background investigation requirements of 10 CFR 73.56.

21. 10 CFR 73.55(g)(7)—Visitors

Guidelines

An acceptable physical security plan would confirm that individuals who have not been granted unescorted access privileges to a protected area or vital areas, but require access for the conduct of authorized activities, are escorted by personnel who are authorized for unescorted access to the area in which the authorized activity will be performed. The plan would also confirm that personnel performing escort duties are knowledgeable of the activities that are authorized to be performed by the individual being escorted.

The physical security plan shall confirm that implementing procedures are in place to address the identification, processing, and escorting of visitors. The security plan should describe the types of personal identification media that will be accepted and the types of visits that will be authorized.

The physical security plan shall confirm that a visitor control register is maintained that includes the name, date, time, purpose of visit, employment affiliation, and citizenship of the visitor, as well as the name of the individual being visited.

The physical security plan shall confirm that a process has been established to verify the true identity of individuals requesting escorted access (visitors), in accordance with the requirements of 10 CFR 73.55(g)(7)(i)(B). Implementing procedures may contain further details.

The physical security plan shall confirm that all visitors are issued and required to wear a identification badge that clearly indicates that an escort is required and that visitors are escorted at all times by personnel who are trained and qualified to perform escort duties in accordance with the requirements specified in 10 CFR 73.55(g)(8).

The physical security plan shall confirm that personnel requesting visitor access to the protected area are not currently denied access to another licensed facility.

22. 10 CFR 73.55(g)(7)(ii)—Non-Employee Personnel Who Require Access

The security plan shall confirm that a process has been implemented for individuals not employed by the licensee but who require frequent or extended unescorted access to the protected area and/or vital areas to perform duties and responsibilities required by the licensee at irregular or intermittent intervals. The security plan should confirm that these individuals will satisfy the access-authorization requirements of 10 CFR 73.56 and 10 CFR 26, and that they shall be issued a non-employee photo identification badge that is easily distinguished from other identification badges before being allowed unescorted access to the protected and vital areas. Non-employee photo-identification badges must visually reflect that the individual is not an employee but that no escort is required.

23. 10 CFR 73.55(g)(8) —Escorts

Guidelines

The physical security plan shall confirm that all escorts are trained to perform escort duties and that personnel escorts are provided with a means of timely communication with security personnel to summon assistance when needed. The security plan should generally describe the types of communication assets that are available for use by personnel escorts, including a description of the location of the assets. The reviewer should determine whether this description supports a conclusion that communication assets meet the "timely communication" requirement of 10 CFR 73.55(g)(8)(ii).

The physical security plan shall confirm that individuals acting as vehicle escorts are trained and qualified in accordance with Section VI of Appendix B to 10 CFR Part 73 and are provided a means of continuous communication with security personnel.

The physical security plan shall describe visitor-to-escort ratios for protected areas and vital areas that are consistent with NRC guidance. Typical visitor-to-escort ratios are 10:1 for the protected area and 5:1 for vital areas. Personnel acting as escorts for visitors must be authorized for unescorted access to areas in which escort duties will be performed and should be generally knowledgeable about the activities that are authorized to be performed by the visitors.

The physical security plan shall confirm that implementing procedures are in place for visitor and vehicle escort, observation, and control. Methods used should be generally addressed in the security plan with more detailed information contained in the implementing procedures.

24. 10 CFR 73.55(h), "Search Programs"

Guidelines

An acceptable physical security plan would describe the search processes implemented at each facility to ensure that unauthorized materials are not allowed to be brought into specified areas of the facility. The security plan shall specify predetermined locations at which required searches will be conducted before granting access to designated facility areas. This description should generally address the actions taken by security personnel to detect, deter, and prevent the introduction of firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage. The reviewer should ensure that the description of search processes is consistent with the type of search being conducted (i.e., personnel, vehicle, or material).

25. 10 CFR 73.55(h)(2)—Owner-Controlled Area Searches

Guidelines

The physical security plan shall specify the use of one or two vehicle-barrier systems at the site. If two vehicle-barrier systems are used (one located in the OCA and one located at the PA perimeter), the licensee shall describe (as applicable) the vehicle search processes that are implemented at the OCA barrier checkpoint(s) and should confirm that site implementing procedures exist for access-control points at OCA barriers. If PA searches are conducted at vehicle-access portals located in the OCA, the security plan shall describe how the integrity of the search is maintained during the movement of the vehicle from the OCA checkpoint to the PA barrier's access portal.

The physical security plan shall specify that areas of the vehicle to be searched include, but are not limited to, the cab, engine compartment, undercarriage, and cargo area.

Where two vehicle-barrier systems are used, the physical security plan shall confirm that two trained and equipped security personnel are used to conduct vehicle searches at the OCA vehicle access-control checkpoint. The security plan shall confirm that at least one armed individual is positioned to observe the search process and provide an immediate response. The security plan should specify the location of this responder in relation to the checkpoint.

The physical security plan shall confirm that all vehicle searches conducted at any vehicle-barrier checkpoint are performed using equipment capable of detecting firearms, explosives, incendiary devices, or other items that could be used to commit radiological sabotage, or by a visual and physical search, or both, to ensure that all potentially hazardous or prohibited items in or attached to the vehicle are clearly identified before access is granted.

The physical security plan shall confirm that all vehicle access-control points are equipped with video surveillance equipment that is monitored by an individual capable of initiating a response, including the location of this individual. The physical security plan should describe the methods used by the licensee to detect attempts to circumvent the vehicle-search process and how this information is transmitted to personnel capable of initiating a response to unauthorized activity.

26. 10 CFR 73.55(h)(3) —Protected-Area Searches

Guidelines

The physical security plan shall confirm that the licensee implements personnel, material, and vehicle search processes to prevent the introduction of firearms, explosives, incendiary devices, or other items that could be used to commit radiological sabotage into the protected area. The physical security plan should confirm that the search for firearms, explosives, incendiary devices, or other items that could be used to commit radiological sabotage is performed using equipment capable of detecting these items, or through visual and physical searches, or both, to ensure that all potentially

hazardous or prohibited items in or attached to the vehicle are clearly identified before access is granted.

The security plan shall describe the conditions under which personnel, vehicles, and materials may be excepted from search requirements and should describe the procedures that will be followed for such instances. This description should address access by local law enforcement personnel, including their vehicles and equipment, by on-duty members of the security force who have exited the PA, and by personnel conducting drills and exercises required by Commission regulations.

The physical security plan shall confirm that implementing procedures are consistent with the manufacturer's specifications for the operation of search equipment and are used to ensure proper performance of the equipment, such as by specifying the removal of outer garments and headgear before entering search-equipment portals. The security plan should describe the processes to be followed when search equipment is not functioning properly or is out of service.

The physical security plan shall confirm that, with the exception of law-enforcement personnel on official duty, all persons are subject to search requirements before access is granted beyond the barrier at which the search is conducted/required. Armed security officers who have been subject to a full protected-area search before reporting for duty but who have exited the protected area in the performance of their official duties may reenter the protected area without being subject to an additional search for firearms.

The physical security plan shall confirm that a visual and physical search is conducted by trained and qualified security officers when search equipment is out of service, not operating satisfactorily, or cannot be used effectively to search individuals.

The physical security plan shall describe the actions to be taken when an attempt to introduce contraband into the protected area is suspected, including communication methods and notifications to be made. This description should generally describe the licensee's policy for detaining an individual or unauthorized material and the applicable state and local laws that govern this policy.

The physical security plan shall confirm that implementing procedures for vehicle searches conducted at vehicle-access portals describe the areas of the vehicle that are searched before access is granted to the protected area.

The physical security plan shall describe the types of exceptions to be granted for materials and should confirm that the specific security measures to be implemented for the excepted items are detailed in facility procedures.

The physical security plan shall confirm that bulk material excepted from protected-area search is escorted by an armed member of the security organization to its final destination or to a receiving area where the excepted items are offloaded and verified. The physical security plan should also confirm that, to the extent practicable, items excepted from the search process are not offloaded adjacent to a vital area, are stored

in locked areas, and have their containers opened by individuals knowledgeable of the contents.

27. 10 CFR 73.55(i), “Detection and Assessment Systems”

Guidelines

An acceptable physical security plan shall describe how detection and assessment systems satisfy the design requirements of 10 CFR 73.55(b) to ensure, at all times, the capability to detect and assess unauthorized persons and support the effective implementation of the site’s protective strategy.

28. 10 CFR 73.55(i)(2)—Intrusion-Detection Equipment

Guidelines

An acceptable physical security plan would confirm that intrusion-detection equipment annunciates, and video assessment equipment displays concurrently, in at least two onsite alarm stations, at least one of which is inside the Protected Area, is bullet-resisting, and has an interior that cannot be viewed from the Protected Area perimeter.

The security plan shall confirm that intrusion-detection equipment must annunciate, and video assessment equipment must display concurrently, in at least two continuously staffed onsite alarm stations, at least one of which must be protected in accordance with the requirements for the central alarm station in 10 CFR 73.55(i). For applicants for a COL or OL, both required alarm stations must meet the requirements for the CAS.

29. 10 CFR 73.55(i)(3)—Design Elements of the Intrusion-Detection and –Assessment Systems

Guidelines

The security plan shall describe the capabilities of the intrusion-detection and assessment systems.

The security plan shall confirm that the intrusion-detection system is designed to: (i) provide visual and audible annunciation of the alarm, (ii) provide a visual display from which assessment of the detected activity can be made, (iii) ensure that annunciation of an alarm indicates the type and location of the alarm, (iv) ensure that alarm devices, including transmission lines to annunciators, are tamper-indicating and self-checking, (v) provide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply, (vi) support the initiation of a timely response in accordance with the security plans, licensee protective strategy, and associated implementing procedures, and (vii) ensure that intrusion-detection and -assessment equipment at the protected area’s perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power.

The physical security program would typically ensure that each intrusion-detection system used at a facility is configured and tested in accordance with the system manufacturer's specifications and the licensee's testing and maintenance procedures.

The physical security plan shall confirm that alarm devices and transmission lines are tamper-indicating and self-checking and provide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on backup power.

The physical security plan shall describe how the intrusion-detection system is used to initiate a timely response in accordance with implementing procedures, the licensee's protective strategy, and communication/notification protocols.

The physical security plan shall confirm that an uninterruptible power supply keeps the intrusion-detection and -assessment equipment at the protected area's perimeter operable during the loss of normal power.

30. 10 CFR 73.55(i)(4)—Alarm Stations

Guidelines

The physical security plan shall confirm that both alarm stations required by 10 CFR 73.55(i)(2) are designed and equipped to ensure that a single act within the capabilities of the design-basis threat addressed in 10 CFR 73.1(a)(1) cannot disable or remove the capabilities of both alarm stations. The physical security plan should generally describe the physical protection program's design features that support a conclusion that in the event of a single act, at least one alarm station will remain operable where personnel can detect and assess alarms, initiate and coordinate an adequate response to an alarm, summon offsite assistance, and provide command and control, and perform other functions required to successfully accomplish the goals and objectives of the site-specific protective strategy.

The physical security plan shall confirm that the central alarm station is located inside a protected area; is bullet-resisting; and has an interior that is not visible from the protected area's perimeter.

The physical security plan shall confirm that both alarm stations are continuously staffed with at least one trained and qualified alarm-station operator and that the alarm-station operator is not assigned other duties or responsibilities which would interfere with their ability to execute the functions required by 10 CFR 73.55(i)(4)(i). The plan shall confirm that other activities within either alarm station that would interfere with an alarm station operator's ability to execute assigned duties and responsibilities are prohibited.

The physical security plan shall confirm that both alarm stations are configured to ensure that both alarm-station operators: can assess and initiate response to all alarms in accordance with the security plans and implementing procedures, as well as other events, as appropriate; cannot change the status of a detection point or deactivate a locking or access-control device at a protected or vital area portal without the knowledge

and concurrence of the alarm-station operator in the other alarm station; are knowledgeable of the final disposition of all alarms; and maintain a written/electronic record of all alarm annunciations, the cause of each alarm, and the disposition of each alarm.

Applicants for an operating license under the provisions of 10 CFR Part 50, or holders of a COL under the provisions of 10 CFR Part 52, s shall confirm in their physical security plan that both the central and secondary alarm stations are constructed, located, protected, and equipped to the standards for the central alarm station contained in 10 CFR 73.55(e)(5) and 73.55(i)(4)(ii)(A). The physical security plan shall also confirm that both alarm stations shall be equivalent and redundant, to the degree that all functions needed to satisfy the requirements of 10 CFR 73.55 for alarm stations can be performed in either alarm station.

31. 10 CFR 73.55(i)(5)—Surveillance, Observation, and Monitoring

Guidelines

An acceptable physical security plan would describe the methods to be used by a licensee to satisfy the surveillance, observation, and monitoring requirements of 10 CFR 73.55, including a description of how these systems are used to identify indications of tampering and are otherwise used to implement the site's protective strategy.

32. 10 CFR 73.55(i)(5)(ii)—Surveillance, Observation, and Monitoring of the Owner-Controlled Area

Guidelines

The physical security plan shall describe the locations (as determined appropriate by the licensee) and methods to be used by the licensee to continuously survey, observe, and monitor the identified OCA locations to detect and deter intruders and to ensure the integrity of physical barriers or other components and functions of the onsite physical protection program.

33. 10 CFR 73.55(i)(5)(iii)—Unattended Openings

Guidelines

The physical security plan shall confirm that unattended openings that intersect a security boundary, such as underground pathways, are protected by a physical barrier and monitored by intrusion-detection equipment or observed by security personnel frequently enough to detect exploitation. The physical security plan should describe the communication methods used to transmit information associated with detection and assessment of unauthorized activities at such locations.

34. 10 CFR 73.55(i)(5)(iv) and (v)—Armed Security Patrols of the Protected Area and Vital Areas

The physical security plan shall confirm that all exterior areas within the protected area are periodically checked by armed security patrols to detect the presence of unauthorized personnel and material, as well as to inspect physical barriers inside the protected area and vital areas and the portals that traverse those barriers. The physical security plan should specify the frequency of protected-area patrols.

35. 10 CFR 73.55(i)(5)(vi)—Random Patrols of Target Sets

The physical security plan shall confirm that all areas containing target sets are patrolled on a random basis. The security plan should specify the frequency of the patrols and the duties and responsibilities of the individual(s) performing the patrols.

36. 10 CFR 73.55(i)(5)(vii)—Tampering

The physical security plan shall confirm that security personnel are trained to recognize obvious signs of tampering in ways consistent with their duties and responsibilities. The physical security plan should describe other training provided to site personnel to assist with identifying and preventing tampering.

37. 10 CFR 73.55(i)(6)—Illumination

Guidelines

An acceptable physical security plan would describe the types of equipment used by the licensee to meet the facility illumination levels required to satisfy the design requirements of 10 CFR 73.55(b) and the implementation of the protective strategy.

The physical security plan shall confirm that the licensee maintains the minimum illumination level of 0.2 foot-candles horizontally at ground level in isolation zones and defined exterior areas within the protected area.

If low-light technology is used to augment lighting to meet lighting requirements, the physical security plan shall describe the facility areas in which the 0.2 foot candle requirement cannot be met; the reasons why the 0.2 foot candle requirement cannot be met; the type of low-light technology used to ensure that observation, surveillance, and assessment requirements can be met; and how this low-light technology is incorporated in the site's protective strategy.

The physical security plan shall confirm that all affected personnel are trained and qualified to perform their assigned duties with assigned equipment under conditions in which the 0.2 foot candle requirement is not met. The plan should also confirm that implementing details are described in facility procedures.

38. 10 CFR 73.55(j), “Communication Requirements”

Guidelines

An acceptable physical security plan would describe the methodology and equipment used by the licensee to maintain a continuous communications capability that will ensure effective command and control with onsite and offsite resources during both normal and emergency situations.

The physical security plan shall confirm that all on-duty security force personnel are capable of maintaining continuous communication with an individual in each alarm station, that vehicle escorts are capable of maintaining continuous communication with security personnel, and that personnel escorts are provided a means of timely communication with security personnel.

The physical security plan shall confirm describe the types of communication systems used, the capabilities of each communication system, and the circumstances under which each communication system will be used to meet Commission requirements. The physical security plan should confirm that the licensee has analyzed site-specific conditions and has identified areas of the facility where communications systems could be interrupted or cannot be maintained. The physical security plan should describe the alternative communication methods or equipment to be used to account for such areas to include confirmation that personnel are trained and qualified to use the alternative communication systems in accordance with implementing procedures.

The physical security plan shall describe how, in addition to the conventional telephone service, the licensee provides continuous communication by establishing radio- or microwave-transmitted two-way voice communication, either directly or through an intermediary, between local law enforcement and the site in both alarm stations, as required by 10 CFR 73.55.

The physical security plan shall confirm that both alarm stations required by 10 CFR 73.55 maintain a means of communication with the control room and should describe the types of communication systems that are used.

The physical security plan shall confirm that an independent/secondary power source is provided for non-portable communications equipment and alarm annunciation equipment in the event of the loss of normal power. The physical security plan should confirm that these independent/secondary power sources are located in a vital area.

The security plan shall confirm that areas of the site have been identified where communications could be interrupted or cannot be maintained, and that alternative communication measures have been established and addressed in facility procedures.

39. 10 CFR 73.55(k), “Response Requirements”

Guidelines

The physical security plan shall confirm that properly trained, qualified, and equipped personnel are available at all times to interdict and neutralize threats, up to and including the DBT of radiological sabotage, as defined in 10 CFR 73.1.

The physical security plan shall confirm that the firearms, ammunition, and equipment necessary to implement the site’s security plans and protective strategy are in sufficient supply and working order and are readily available to security personnel. The physical security plan should describe the firearms, ammunition, and equipment necessary to implement the site’s security plans and protective strategy.

The physical security plan shall confirm that each armed member of the security organization is trained to prevent or impede attempted acts of radiological sabotage by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or under any other circumstances, as authorized by applicable State or Federal law.

The physical security plan shall describe the duties and responsibilities of the security personnel used as armed responders and armed security officers to implement the site’s protective strategy within predetermined timelines.

For sites that use a remotely operated weapons system (ROWS), the physical security plan should also describe the duties and responsibilities of the ROWS operators, including operator actions and capabilities in the event that the ROWS becomes inoperable during a contingency event.

The number of armed responders designated to implement the protective strategy shall not be fewer than 10, and the number of armed responders for the site shall be documented in the physical security plan.

The physical security plan shall confirm that the number of armed responders is sufficient to effectively implement the protective strategy, that they are available at all times inside the protected area (which may include the protected area’s access-control point), and that they are not assigned other duties or responsibilities that could interfere with their assigned response duties.

The physical security plan shall confirm that armed security officers designated to strengthen the onsite response are onsite and available at all times to carry out their assigned duties. The number of armed security officers designated to implement the protective strategy for the site shall be documented in the physical security plan.

For sites that use ROWS, the physical security plan should describe the number of ROWS employed at the site and the number of ROWS operators required to operate

these systems (e.g., the system-to-operator ratio), in a way consistent with the implementation of the site's protective strategy. The licensee should also describe the integration of the ROWS with the site's protective strategy, specifically stating whether these systems and the system operators are designated as a component of the minimum number of armed responders or of the armed security officers in the site's protective strategy.

The physical security plan should identify the number of armed security shift supervisors who may use the force continuum, including the use of deadly force, as authorized by applicable State law, for targets of opportunity and self-defense when implementing the site's protective strategy. If the licensee's physical security plan identifies armed security shift supervisors, these individuals must also be trained and qualified to perform armed duties in support of security-related and contingency events. For further information on armed security shift supervisors, see NRC Staff White Paper "Duties and Responsibilities of the Security Shift Supervisor for Power Reactor Licensees," dated August 2009, available (though not publicly) as Agencywide Documents Access and Management System (ADAMS) Accession No. ML100760663.

The physical security plan shall confirm that facility procedures provide a process to reconstitute the documented number of available armed response personnel required to implement the protective strategy. The physical security plan should document a specified timeframe to re-establish the minimum number of available armed response personnel.

40. 10 CFR 73.55(k)(8)—Protective Strategy

Guidelines

The physical security plan shall confirm that a written protective strategy is established that provides the methodology of the site's protective strategy to account for and protect the personnel, systems, and equipment needed to prevent significant core damage and spent-fuel sabotage.

The physical security plan shall confirm that, upon receipt of an alarm or other indication of a threat, the licensee has pre-established methodologies and procedures to determine the existence and level of the threat and that facility procedures provide the details of this process.

The physical security plan shall confirm that response actions are initiated to interdict and neutralize threats in accordance with the requirements of 10 CFR Part 73, Appendix C, Section II, the safeguards contingency plan, and the site's protective strategy.

The physical security plan shall confirm that local law enforcement is notified in accordance with facility procedures.

The protective strategy shall meet the requirements of Section II of Appendix C to 10 CFR Part 73.

41. 10 CFR 73.55(k)(9)—Law-Enforcement Liaison

Guidelines

The physical security plan shall describe the process of documenting and maintaining the current agreements with local, State, and Federal law enforcement, including the estimated response times and the capabilities of the applicable law-enforcement agencies. To the extent practicable, documentation of the law-enforcement agreements should also include the number of personnel for response, available weapons, marshaling locations, command and control protocols, and frequency of training for law-enforcement personnel contained in the site law enforcement response plan.

42. 10 CFR 73.55(k)(10)—Heightened Security

Guidelines

The physical security plan shall confirm that a threat warning system is established, maintained, and implemented which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat. The security plan shall confirm that these measures and actions are consistent with the security plans and other emergency plans and procedures. The security plan shall confirm that, upon notification by an authorized representative of the Commission, licensees shall implement the specific threat level indicated by the Commission representative.

43. 10 CFR 73.55(l), “Facilities Using Mixed-Oxide (MOX) Fuel Assemblies Containing up to 20 Weight Percent Plutonium Dioxide (PuO2)”

Guidelines

The physical security plan should address the use of mixed-oxide (MOX) fuel assemblies containing up to 20 weight percent plutonium dioxide and the associated requirements for physical security systems, operational requirements, and management systems for possession, storage, and transport of such assemblies, as well as the corresponding requirements for MOX fuel assemblies exceeding 20 weight percent PuO_2.

For further details, see RG 5.78, “Protection of Mixed Oxide Fuels in Nuclear Power Plants,” ADAMS Accession No. ML13151A355. (This document is not publicly available.)

44. 10 CFR 73.55(m), “Security Program Reviews”

Guidelines

The physical security plan shall address the use of security programs, including the requirements for implementation of reviews, documentation, and reporting.

The physical security plan shall confirm that a review of the security program is conducted for each element of the program at least every 24 months.

The physical security plan shall confirm that a security-program review is conducted within 12 months after initial implementation or when a change in personnel, procedures, equipment, or facilities could adversely affect security.

The physical security plan shall confirm that the security-program review is completed by personnel who are independent of those responsible for program management and of any individual who has direct responsibility for implementing the onsite physical protection program.

The physical security plan shall confirm that the review of the security program, at a minimum, includes an audit of the effectiveness of the physical security program; security plans; implementing procedures; cyber security program; safety and security interface activities; the testing, maintenance, and calibration program; and response commitments by local, State, and Federal law enforcement agencies.

The physical security plan shall confirm that the results and recommendations of the reviews of the onsite physical protection program, management findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews are documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operations. The security plan shall confirm that these reports are kept in an auditable form and available for inspection.

The physical security plan must confirm that findings from onsite physical protection program reviews must be entered into the site's corrective-action program.

45. 10 CFR 73.55(n), "Maintenance, Testing, and Calibration"

Guidelines

The physical security plan shall address maintenance, testing, and calibration of physical security systems and equipment on a predetermined schedule to maintain operable conditions for, and capabilities of, performing intended functions; procedures include criteria for determining problems, failures, deficiencies and other findings; documentation and tracking in the site's corrective-action program for resolution; implementation of compensatory measures; and specific systems-testing requirements.

The physical security plan shall describe a maintenance, testing, and calibration program to ensure that security systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, are kept in an operable condition, and are capable of performing their intended function.

The physical security plan shall describe that implementing procedures specify the operation and technical details required to perform maintenance, testing, and calibration activities. Site maintenance, testing, and calibration procedures identify the criteria for determining when problems, failures, deficiencies, and other findings are documented in the site's corrective-action program for resolution.

The physical security plan shall confirm that effective compensatory measures are implemented when there is a failure or degraded operation of security-related components or equipment.

The physical security plan shall confirm, at a minimum, that intrusion-detection and -assessment equipment, access-control equipment, communications equipment, search equipment, security personnel's equipment, firearms, and active vehicle-barrier systems are tested and maintained as part of the site's maintenance, testing, and calibration program.

The physical security plan shall confirm that each intrusion alarm is tested for operability at the beginning and end of any period that it is used for security. If the period of continuous use is longer than 7 days, the intrusion alarm should be tested at least once every 7 days.

The physical security plan shall confirm that onsite communications equipment is kept in operational condition and tested for operability at least once at the beginning of each security-personnel work shift.

The physical security plan shall confirm that equipment required for communications between alarm stations, each control room, and local law-enforcement agencies, as well as backup communications equipment, is tested at least once each day.

The physical security plan shall describe how search equipment is kept in operational condition and is tested for operability at least once each day and tested for performance at least once during a 7-day period.

The physical security plan shall confirm that security personnel's equipment is kept in an operable condition with equipment checks or inspections to ensure that the equipment can perform the intended function.

The physical security plan shall confirm that a firearms maintenance program is established that includes the maintenance, testing, and accountability of all assigned licensee firearms. The physical security plan shall also confirm that the firearms maintenance program includes semiannual test firing for accuracy and functionality; firearms maintenance procedures that include cleaning schedules and cleaning requirements; program activity documentation; control of and accountability for weapons and ammunition; firearms storage requirements; and armorer certification.

For sites that use an ROWS, the physical security plan shall confirm that the system components and associated firearms are included in the firearms maintenance program

and that, at a minimum, the system is maintained, tested, calibrated, and the weapon test-fired in accordance with the requirements of Section VI.G.3 of Appendix B to 10 CFR Part 73, , licensee procedures, and manufacturer's specifications.

The physical security plan shall confirm that the active vehicle-barrier systems employed by the licensee, including associated backup power supplies, are kept in an operable condition and are tested in accordance with licensee procedures.

The physical security plan shall confirm that facility implementing procedures describe a program for testing or verifying the operability of devices or equipment located in hazardous areas, or that alternative measures are taken to ensure timely completion, or that testing or maintenance is conducted when hazardous conditions or other restrictions are no longer applicable.

46. 10 CFR 73.55(o), "Compensatory Measures"

Guidelines

The physical security plan shall identify the criteria for instituting compensatory measures when security equipment, systems, or components become degraded or inoperable. The plan shall also identify the specific measures that provide a level of protection equivalent to that of the degraded or inoperable equipment, systems, and components.

The physical security plan shall identify the specific timeframe for implementing compensatory measures to ensure that degraded conditions do not decrease the effectiveness of the physical security program and protective strategy and continue to meet the general performance objective of 10 CFR 73.55(b).

47. 10 CFR 73.55(p), "Suspension of Security Measures"

Guidelines

The physical security plan must describe the process for the suspension of security measures. The process described in the security plan shall include the criteria within the provisions of 10 CFR 73.55(p) and 10 CFR 50.54(x) and (y).

48. 10 CFR 73.55(q), "Records"

The physical security plan shall confirm that records on these documents are maintained in a way consistent with 10 CFR 73.55(q) and 10 CFR 73.70: access-authorization records, suitability records, physical and mental qualification records for security personnel, protected-area visitor access records; protected-area vehicle access records; vital-area access transactions; vitalization and devitalization records; vital-area access list reviews; security plans and procedures; records of security patrols; inspection, tests, and maintenance records; alarm annunciation and security responses; records of liaison with local law-enforcement agencies; records of audits and reviews; records of security-related access-control devices; security training and qualification records; weapons

testing, maintenance, and accountability records; the engineering analysis for the vehicle-barrier system; and work-hour control records.

The security plan shall describe the retention timeframe for records to be kept in accordance with 10 CFR 73.55(q).

If a contracted security force is used at the site, the written contract agreements must be retained as a record for the duration of the contract.

The engineering analysis for the site's vehicle-barrier system(s) should be retained for the duration of the operating license.

49. 10 CFR 73.55(r), "Alternative Measures"

Guidelines

The provision for alternative measures in 10 CFR 73.55(r) requires that, before implementation, these measures be submitted for NRC review and approval, in accordance with 10 CFR 50.4, "Written Communications," and 10 CFR 50.90, "Application for Amendment of License, Construction Permit, or Early Site Permit."

The physical security plans shall indicate when a specific measure described in the plan is an alternative measure and should indicate that the measure has been reviewed and approved by the NRC in accordance with 10 CFR 73.55(r) and 10 CFR 50.90.

50. 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Reactors"

Guidelines

See review guidance described in SRP 13.6.4, "Access Authorization - Operational Program" (ADAMS Accession No. ML12125A098), for staff technical review and RG 5.66, "Access Authorization Program for Nuclear Power Plants" (ADAMS Accession No. ML13151A355, but not publicly available) for acceptable methods and approaches for meeting regulatory requirements.

The physical security plans shall describe the operational requirements, management systems, and organization in sufficient details for how requirements for personnel access to a nuclear power plant will meet the criteria in 10 CFR 73.56(a) through 73.56(o). The reviewer should apply the staff guidance provided in SRP 13.6.4 for the technical review of access authorization and RG 5.66, "Access Authorization Program for Nuclear Power Plants," for acceptable methods and approaches for meeting regulatory requirements. The descriptions provided and the level of detail for describing the personnel access authoraciaton should conform to SRP 13.6.4.

51. 10 CFR 73.57, “Requirements for Criminal History Records Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility, a Non-Power Reactor, or Access to Safeguards Information”

Guidelines

The physical security plans shall describe the operational requirements, management systems, and organization for how requirements for criminal history record checks will be performed prior to granting unescorted personnel access of individual unescorted access to the vital and protected areas of nuclear power plant. The plan shall also describe how processes and procedures for implementing criminal background checks prior to allowing individual accessing to safeguards information. The descriptions should be sufficient to indicate in sufficient the detail of how process and procedures that implement these requirements and indicate that details will be captured in plant policy and operational procedures for the conduct of security operations.

52. 10 CFR 73.58, “Safety/Security Interface Requirements for Nuclear Power Reactors”

Guidelines

The physical security plans reference the Final Safety Analysis Report, Chapter 13, Conduct of Operations, that describe the operational requirements, management systems, and organization provide sufficient details for how requirements for safety/security interface will be address for conducting plant operations. The descriptions of management systems should conform to RG 5.74 for managing the safety/security interface for acceptable licensing bases satisfying the criteria set forth in 10 CFR 73.58. RG 5.74, *“*Managing the Safety/Security Interface” (ADAMS Accession No. ML091690036), describes acceptable methods and approaches for meeting regulatory requirements.

53. 10 CFR 73.70, “Records”

Guidelines

The physical security plan shall describe that detailed procedures will be established to comply with requirements of each prescriptive requirements of 10 CFR 73.70 (i.e., each record must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period). The detailed procedures developed will include compliance with storage requirements (i.e., the record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, and specifications must include all pertinent information such as stamps, initials, and signatures). The physical plan shall indicated that record processes and procedures included adequate safeguards against tampering with and loss of records.

54. 10 CFR 73.71, “Reporting of Safeguards Events”

Guidelines

The physical security plan shall describe that detailed procedures will be established for reporting of safeguards events. The detailed procedures will include notifying the NRC Operations Center through the Emergency Notification System within one hour after discovery of the loss of any shipment of SNM or spent fuel, and within one hour after recovery of or accounting for such a lost shipment and provisions to maintain an open and continuous communication channel with the NRC Operations Center. The procedures established include the initial telephonic notification must be followed within a period of 60 days by a written report submitted to the NRC by an appropriate method listed in 10 CFR 73.4, and one copy of the written report addressed to the Director, Division of Security Policy, Office of Nuclear Security and Incident Response, and the standard for report that include sufficient information for NRC analysis and evaluation.

55. 10 CFR 73.75, “Posting”

Guidelines

The physical security plan shall describe that detailed procedures will be established for posting required for compliance with 10 CFR 73.75. The detailed procedure for posting shall include, at a minimum compliance with requirements that a protected area shall conspicuously post notices at every vehicle and pedestrian entrance to the protected area, Also Licensees or certificate holders operating facilities that include buildings that are not within a protected area but nonetheless contain special nuclear material, byproduct material, or source material shall conspicuously post notices at the personnel and vehicle entrances to each such building.

56. Appendix G to Part 73, “Reportable Safeguards Events”

Guidelines

The physical security plan shall describe that detailed procedures will be established for reporting and include the events described in Appendix G to Part 73. At minimum, the security plant states that detailed procedures for reporting safeguards events under the following criteria:

A. events to be reported within one hour of discovery, followed by a written report within 60 days

(i) any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause:

a) a theft or unlawful diversion of special nuclear material

b) significant physical damage to a power reactor or any facility possessing SSNM or its equipment or carrier equipment transporting nuclear fuel or spent nuclear fuel, or to the nuclear fuel or spent nuclear fuel a facility or carrier possesses

c) interruption of normal operation of a licensed nuclear power reactor through the unauthorized use of or tampering with its machinery, components, or controls, including the security system

(ii) an actual entry of an unauthorized person into a protected area, material access area, controlled access area, vital area, or transport

(iii) any failure, degradation, or discovered vulnerability in a safeguard system that could allow unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or transport for which compensatory measures have not been employed

(iv) the actual or attempted introduction of contraband into a protected area, material access area, vital area, or transport

B. events to be recorded within 24 hours of discovery in the safeguards event log

(i) any failure, degradation, or discovered vulnerability in a safeguards system that could have allowed unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or transport had compensatory measures not been established

(ii) any other threatened, attempted, or committed act not previously defined in Appendix G with the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of such reduction in effectiveness

Training and Qualification Plan

In accordance with 10 CFR 73.33(c)(4), which states that "[t]raining and Qualification Plan. The licensee shall establish, maintain, and implement, and follow a Training and Qualification Plan that describes how the criteria set forth in appendix B, section VI, to this part, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," will be implemented," the T&QP shall describe the how the requirements for selecting, training, equipping, testing, and qualifying individuals who are responsible for the protection of special nuclear materials, nuclear facilities, and nuclear shipments, and personnel who perform security duties, are met. In summary the T&QP descriptions should be sufficient detailed to address the following:

A. The standards and criteria required for security personnel, in accordance with requirements of Section VI of Appendix B to 10 CFR Part 73;

B. The requirements for (1) security personnel, including how they will be selected, trained, equipped, tested, and qualified for specific defined roles and responsibilities for security functions protecting the activities involving special nuclear materials, nuclear facilities, and nuclear shipments, and (2) personnel who perform security duties;

C. The methods and approaches for training and qualification of security personnel to perform required security functions, which may conforms to that described in RG 5.75;

D. The site specific training and qualification that support the assumptions and requirements in the licensing bases for the design of a physical protection system and meet the specifics (e.g., timelines, minimum distances for line of fire, proficiencies in use of firearms, etc.) for the reliability and availability of capabilities to perform required interdiction and neutralize DBT adversaries.

Applicants and power reactor licensees subject to the requirements of 10 CFR 73.55 shall comply only with the requirements of Section VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," of Appendix B to Part 73. All other licensees, applicants, or certificate holders shall comply only with Sections I through V of Appendix B to Part 73.

1. Section VI(A) "General Requirements and Introduction," of Appendix B to 10 CFR Part 73

Guidelines

An acceptable Security Training and Qualification Plan (T&QP) would describe how all individuals who are assigned duties and responsibilities are required to: implement the Commission-approved security plans; prevent significant core damage and spent-fuel sabotage; implement the licensee protective strategy; implement facility security procedures; and be trained and qualified in accordance with minimum training and qualification requirements for the assigned duties and responsibilities to ensure that each individual possesses the knowledge, skills, and abilities (KSAs) required to effectively perform the assigned security-program duties and responsibilities.

The T&QP shall confirm that the licensee selection and re-evaluation process has a methodology for ensuring that all personnel performing the security program's required duties, responsibilities, and functions are properly suited, trained, equipped, and qualified to perform their assigned duties, responsibilities, and functions and should describe how the licensee will ensure that these personnel meet the Commission-developed minimum training and qualification requirements contained in Section VI of Appendix B to 10 CFR Part 73, including the processes by which all individuals will be selected, trained, equipped, tested, and qualified.

The T&QP shall describe the process to be used by a licensee to demonstrate that all personnel possess the KSAs required to effectively perform their assigned duties and responsibilities before individuals are assigned those duties or responsibilities.

The T&QP shall confirm that the training and qualification program simulates, as closely as practicable, the specific conditions under which the individual shall be required to perform assigned duties and responsibilities and that individuals will not be permitted to perform security functions, assume security duties or responsibilities, or return to security duty until that individual satisfies the training and qualification requirements of Section VI of Appendix B to 10 CFR Part 73 and the Commission-approved training and qualification plan, unless specifically authorized by the Commission.

The T&QP shall confirm that annual training will be scheduled nominally, within a 12-month period after the date on which initial training was completed, with an allowance of up to 3 months before or 3 months after the scheduled date. Given this allowance, the next annual training must continue to be scheduled 12 months from the initial or previously scheduled date, rather than from the earlier or later date that the training was actually completed. This allowance is intended to provide a level of flexibility to the licensee and security personnel to account for unforeseen circumstances without creating a situation in which the annual date is continuously changing from year to year.

2. Section VI(B)(1), "Suitability," of Appendix B to 10 CFR Part 73

Guidelines

An acceptable T&QP would confirm that the licensee selection and re-evaluation process has a methodology for ensuring that individuals who are assigned security duties and responsibilities meet minimum requirements for initial and continued suitability (i.e., acceptability). The training and qualification plan shall describe how the licensee will ensure that each member of the security organization is, and continues to be, qualified (i.e., proven capable) to provide the required services both before employment and during assignment to the security organization.

The T&QP shall confirm that all individuals employed by the security organization or assigned security-program duties, in either armed or unarmed positions, meet the requirements for suitability under Section VI.B.1 of Appendix B to 10 CFR Part 73.

3. Section VI.B.2, "Physical Qualifications," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall confirm that the licensee selection and re-evaluation process has a methodology for ensuring that personnel assigned security duties and responsibilities do not have any physical conditions that would adversely affect their performance of those duties and responsibilities and that those personnel must demonstrate, before their employment by and during their assignment to the security organization, the necessary physical qualifications to effectively perform those assigned duties.

4. Sections VI.B.2(a)(2) through VI.B.2(f) of Appendix B to 10 CFR Part 73—Medical Examinations and Physical Qualifications

Guidelines

The training and qualification plan shall confirm that the licensee selection and re-evaluation process has a methodology for ensuring that armed and unarmed individuals assigned security duties and responsibilities are subject to a physical examination designed to measure the individual's physical ability to perform assigned duties and responsibilities.

The training and qualification plan shall confirm that physical examinations are administered by a licensed health professional, with the final determination being made by a licensed physician, to verify the individual's physical capability to perform assigned duties and responsibilities.

The training and qualification plan shall confirm that both armed and unarmed individuals who are assigned security duties and responsibilities identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures meet the minimum physical requirements of Appendix B to 10 CFR Part 73 in Sections VI.B.2(b) for vision, VI.B.2(c) for hearing, VI.B.2(d) for existing medical conditions, VI.B.2(e) for addiction, and VI.B.2(f) if they are returning to duty from incapacitation caused by illness, injury, disease, or an operation.

5. Section VI.B.3, "Psychological Qualifications," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall confirm that the licensee selection and re-evaluation process has a methodology for ensuring that security personnel meet the psychological qualifications of Section VI.B.3 of Appendix B to 10 CFR Part 73. It shall also confirm that a licensed psychologist, psychiatrist, or physician trained, in part, to identify emotional instability has the responsibility to determine whether armed members of the security organization and alarm station operators have an emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

6. Section VI.B.4, "Medical Examinations and Physical Fitness Qualifications," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall confirm that the licensee selection and re-evaluation process has a methodology for ensuring that armed members of the security organization are subject to a medical examination by a licensed physician to determine if the individual is fit to participate in physical fitness tests.

The training and qualification plan shall confirm that the licensee selection and re-evaluation process has a methodology for ensuring that, before assignment, armed

members of the security organization demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test.

The training and qualification plan shall confirm that the licensee's physical fitness test includes site-specific physical conditions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security duties, that regularly exist at the site during both normal and emergency operations, and that the test simulates site-specific conditions under which the individual will be required to perform their assigned duties and responsibilities.

The training and qualification plan shall describe the physical fitness test administered at the site in a manner that demonstrates that the test includes strenuous activity, physical exertion, levels of stress, and exposure to the elements and that it simulates site-specific conditions.

A. The T&QP shall provide a general description of the Licensee's Physical Fitness test and how the strength, endurance, and agility requirements are demonstrated.

B. The T&QP should confirm that site-specific conditions are addressed in site procedures.

Section C.2.9, "Medical Examinations and Physical Fitness Test," of Regulatory Guide 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities" (ADAMS Accession No. ML091690037) contains additional details.

7. Section VI.B.5, "Physical Requalification," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall confirm that the licensee has a methodology for ensuring that armed and unarmed individuals demonstrate the capability to meet the physical requirements of Section VI of Appendix B to 10 CFR Part 73 and of the licensee training and qualification plan at least annually and that requalification is documented by a qualified training instructor and attested to by a security supervisor.

8. Section VI.C.1, "Duty Training," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall confirm that the licensee implements a methodology for ensuring that all personnel who are assigned to perform any security-related duty or responsibility are trained and qualified to perform assigned duties and responsibilities to ensure that each individual possesses the minimum KSAs required to effectively carry out those assigned duties and responsibilities.

The training and qualification plan shall confirm that individuals performing security duties are trained to perform assigned duties and responsibilities and meet the minimum

qualification requirements of Section VI of Appendix B to 10 CFR Part 73 and the licensee training and qualification plan.

The training and qualification plan shall confirm that individuals performing security duties are trained and qualified in the use of all equipment or devices required to effectively perform all assigned duties and responsibilities.

The training and qualification plan shall contain a list of critical job-task KSAs for which individuals assigned to perform security duties must be trained and qualified. This listing should identify the specific duty positions within the security organization and the specific jobs for which individuals in each duty position are to be trained and qualified. The specific duty positions identified on the critical job-task list shall remain consistent between the PSP, T&QP, and SCP.

The critical job-task list (critical task matrix) should provide a method of verification for the training and qualification that the individual in each duty position within the security organization is required to complete, along with the frequency of requalification and the specific method to be used for the qualification or requalification. The critical task matrix should be consistent with the training and qualifications required for the performance of specific security duties (e.g., armed security officers who are designated as a component of the protective strategy should be trained and qualified to respond to contingency events). Section C.3, "Individual Training and Qualification for Duty," of Regulatory Guide 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities" (ADAMS Accession No. ML091690037), provides additional details concerning the list of job tasks for the training and qualification plan.

9. Section VI.C.2, "On-the-Job Training," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall confirm that the licensee implements a methodology for ensuring that individuals assigned duties to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures are provided on-the-job training (OJT) before performing their assigned duties.

The training and qualification plan shall confirm that the methodology used requires each individual to complete a minimum of 40 hours of OJT to demonstrate the KSAs required to effectively perform assigned contingency duties and responsibilities in accordance with the safeguards contingency plans, protective strategy, and implementing procedures. The training and qualification plan should also confirm that OJT is documented by a qualified training instructor and attested to by a security supervisor.

The training and qualification plan shall confirm that the methodology used to ensure that each individual receives the minimum OJT for contingency activities and drills includes, but is not limited to, hands-on application of KSAs related to:

- response-team duties
- use of force

- tactical movement
- cover and concealment
- defensive positions
- fields of fire
- redeployment
- communications (primary and alternative)
- use of assigned equipment
- target sets
- tabletop drills
- command and control duties
- the licensee's protective strategy

10. Section VI.C.3, "Performance Evaluation Program," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall confirm that the licensee has developed, implements, and maintains a performance-evaluation program that is documented in procedures. The training and qualification plan should describe how the licensee will demonstrate and assess, through the performance-evaluation program, the effectiveness of its onsite physical protection program and protective strategy, including the capability of the armed response team to carry out its assigned duties and responsibilities during safeguards contingency events.

The training and qualification plan should confirm that the performance-evaluation program includes procedures for the conduct of tactical response drills and force-on-force exercises designed to demonstrate and assess the effectiveness of the licensee's physical protection program, protective strategy, and contingency event response by all individuals with responsibilities for implementing the safeguards contingency plan and protective strategy.

The training and qualification plan shall confirm that tactical response drills and force-on-force exercises are designed to challenge the site's protective strategy against elements of the DBT and should describe the methodology used to ensure that each participant assigned security duties and responsibilities demonstrates the requisite KSAs.

The training and qualification plan shall confirm that the licensee implements a methodology for ensuring that tactical response drills, force-on-force exercises, and associated contingency response training are conducted under conditions that simulate, as closely as practicable, the site-specific conditions under which each member will, or may, be required to perform assigned duties and responsibilities.

The training and qualification plan shall confirm that tactical response drills and force-on-force exercises include a documented post-exercise critique in which participants identify failures, deficiencies, or other findings related to performance, plans, equipment, or strategies.

The training and qualification plan shall confirm that the licensee documents scenarios and participants for all tactical response drills and annual force-on-force exercises.

The training and qualification plan shall confirm that the licensee implements a methodology for ensuring that findings, deficiencies, and failures identified during tactical response drills and force-on-force exercises that adversely affect or decrease the effectiveness of the protective strategy and physical protection program are entered into the licensee's corrective-action program to ensure that timely corrections are made to the appropriate program areas.

The training and qualification plan shall confirm that, during the conduct of tactical response drills and force-on-force exercises, only the total number of armed responders and designated armed security officers documented in the security plan are used; that artificialities are minimized; that systems or methodologies for the simulation of armed engagement are used; and that each scenario used provides a credible realistic challenge to the protective strategy and response organization.

The training and qualification plan shall confirm that the performance-evaluation program is designed to ensure that: each member of each shift who is assigned duties and responsibilities required to implement the safeguards contingency plan and licensee protective strategy participates in at least one tactical response drill on a quarterly basis and one force-on-force exercise on an annual basis; the mock adversary force replicates the adversary characteristics and capabilities of the DBT as closely as possible and is capable of challenging the licensee's protective strategy; protective strategies can be evaluated by conducting tabletop drills; and drill and exercise controllers are trained and qualified to possess the requisite knowledge to control drills and exercises.

The training and qualification plan shall confirm that the licensee has developed and documented multiple scenarios for tactical response drills and force-on-force exercises; that the scenarios are designed to test and challenge any components or a combination of components of the physical protection program and protective strategy; and that each scenario uses a unique target set or target sets and adversary characteristics, so that all components of the physical protection program and protective strategy are challenged, including but not limited to equipment, implementing procedures, and personnel. The training and qualification plan should confirm that the licensee has implemented procedures to oversee the frequency at which developed scenarios are used to include the conditions under which a single scenario may be repeated. The frequent or repeated use of any one scenario should be avoided as such repletion will diminish the ability of the scenario to challenge response personnel as well as the protective strategy.

11. Section VI.D, "Duty Qualification and Requalification," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall confirm that armed and unarmed individuals are required to demonstrate the required KSAs necessary to carry out assigned duties and responsibilities, as stated in the Commission-approved security plans, the licensee's protective strategy, and implementing procedures. The T&QA plan shall also confirm

that this demonstration includes the achievement of minimum scores on written exams and the observation of hands-on performance by qualified instructors.

The training and qualification plan shall confirm that written exams are administered, and should describe the evaluation criteria that are used for written exams as well as the criteria used to conduct and evaluate performance demonstrations.

The training and qualification plan shall confirm that written exams are administered annually to armed members of the security organization and that this annual written exam is designed to demonstrate that each armed member of the security organization possesses the required KSAs needed to carry out their assigned duties and responsibilities.

The training and qualification plan shall provide a description of the annual written exam. This description should confirm that personnel must achieve a minimum score of 80 percent on the annual written exam to demonstrate an acceptable understanding of assigned duties and responsibilities and should be consistent with RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities." At a minimum, this description should include these elements and evaluation criteria:

- role of security personnel in supporting the safe operation of the facility
- use of deadly force, including the principals involved in the application, escalation, and de-escalation of force
- 10 CFR Part 73 requirements for the protection of SGI
- authority of private security personnel
- knowledge of who has the power of arrest and the authority to detain
- authority to search individuals and seize property
- offsite law enforcement response
- tactics and force that an adversary group might use to achieve its objectives
- response force deployment, tactical movement withdrawal, and use of support fire

The training and qualification plan shall confirm that armed and unarmed individuals are requalified at least annually. The training and qualification plan should confirm that the results of each initial qualification and recurring requalification are documented by a qualified training instructor and attested to by a security supervisor.

12. Section VI.E, “Weapons Training,” of Appendix B to 10 CFR Part 73

General Firearms Training

Guidelines

The training and qualification plan shall describe the weapons training program and, within this description, should confirm that each armed member of the security organization is trained and qualified by a certified firearms instructor in the use and maintenance of each assigned weapon, including but not limited to marksmanship, assembly, disassembly, cleaning, storage, handling, clearing, loading, unloading, and reloading for each assigned weapon. The training and qualification plan shall confirm that the licensee conducts annual firearms familiarization in accordance with a nationally recognized or law-enforcement-approved course of fire.

The training and qualification plan shall confirm that firearms training is conducted by firearms instructors that are certified by a recognized national or State entity and that the certified firearms instructors are recertified in accordance with the standards recognized by the certifying national or State entity. The training and qualification plan shall describe how often firearms instructors are recertified and shall confirm that under no circumstances will instructors be recertified less often than once every 3 years.

At a minimum, the training and qualification plan shall confirm that the licensee’s firearms training program includes:

- mechanical assembly and disassembly, weapons capabilities, and fundamentals of marksmanship
- cleaning and storage
- combat firing, day and night
- safe weapons handling
- clearing, loading, unloading, and reloading
- firing under stress
- zeroing duty weapon(s) and weapons sighting adjustments
- target identification and engagement
- weapon malfunctions
- cover and concealment
- weapons familiarization

Where a licensee has chosen to use a remotely operated weapons system (ROWS), the training and qualification plan shall confirm that the licensee has incorporated training and qualification standards, criteria, and processes that are specific to the use of ROWS, and that ROWS operators are provided training within the elements identified above as they apply to the manufacturer's specifications for the ROWS and training with the specific firearm deployed by the ROWS as applicable.

The training and qualification program shall confirm that armed members of the security organization are instructed on the use of deadly force, as authorized by applicable State law.

The training and qualification plan shall describe firearms training activities that are required by the licensee and how often the licensee will perform these firearms training activities. The training and qualification shall confirm that each armed member of the security organization is required to perform firearms training activities at intervals nominally every 4 months. Where a licensee chooses to incorporate schedule flexibility into their training and qualification program, the training and qualification plan shall specify the flexibility that is used. Where flexibility is incorporated, the training and qualification plan shall specify that firearms training activities are required to be conducted nominally every 4 months with an allowance of up to, but not exceeding, 5 weeks before and 5 weeks after the scheduled date. The training and qualification plan shall confirm that, if flexibility is used, the next scheduled date must be 4 months from the originally scheduled date and not the date on which the training was physically performed.

13. Section VI.F, "Weapons Qualification and Requalification Program," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan shall describe the methodology used to ensure that all armed members of the security organization are qualified and requalified on assigned weapons.

The training and qualification plan shall list the courses of fire and minimum scores that must be achieved by each armed member of the security organization to demonstrate proficiency for each assigned weapon used at the site. The training and qualification plan shall confirm that the results of weapons qualification and requalification are documented and retained as a record, including the minimum length of time that such records must be retained. At a minimum, the training and qualification plan shall confirm that:

- Each course of fire used to meet Commission requirements for firearms qualification and requalification of armed members of the security organization is specific to each type of firearm (to include ROWS as applicable) used at the facility and is in accordance with the standards and

criteria established by a law enforcement agency's course of fire or an equivalent nationally recognized course of fire.

- The annual daylight qualification and requalification courses of fire require that each armed member of the security organization demonstrate a minimum qualifying score of 70 percent with a handgun and shotgun and a minimum score of 80 percent with a semiautomatic rifle or (if used) enhanced weapons. For sites that use ROWS, the minimum score should be specific to the category of firearm used (i.e., semiautomatic rifle or enhanced weapon (as applicable).

- The annual night-fire qualification and requalification courses of fire require that each armed member of the security organization demonstrate a minimum qualifying score of 70 percent with a handgun and shotgun and a minimum score of 80 percent with a semiautomatic rifle or (if used) enhanced weapons. For sites that use ROWS, the minimum score should be specific to the category of firearm used (i.e., semiautomatic rifle or enhanced weapon (as applicable).

For tactical weapons qualification and requalification courses of fire, the training and qualification plan should describe the types of firearms used, the types of actions or activities that are required to be performed as identified by the firearms qualification program, and other tactical training required to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures. Licensee-developed tactical qualification and requalification courses of fire must describe the performance criteria to be met, to include the site-specific conditions (e.g., lighting, elevation, and fields of fire) under which assigned personnel are required to carry out their assigned duties.

The training and qualification plan should confirm that the qualifying score for the annual tactical qualification and requalification course of fire must be an accumulated total of 80 percent of the maximum obtainable score.

To be consistent with RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities," the training and qualification plan should confirm that the licensee's tactical qualification and requalification course of fire include, at a minimum:

- the combined use of handguns and shoulder-fired weapons employed during a contingency event, according to the site's protective strategy

- firing from a reasonable and representative facsimile of licensee defensive positions, elevations, and distances

- appropriate levels of stress and physical demands (e.g., engaging targets while on the move)

- proper cover and concealment tactics while engaging multiple targets, moving targets, and decision-making targets

- the ability to make the transition from one type of firearm to another
- the ability to recover from simulated weapon malfunctions (e.g., dummy rounds)
- adherence to the safe handling of firearms during simulated courses of fire
- firing at multiple targets, loading, and reloading while wearing a protective mask (gas mask)
- no dominant (support) hand shooting
- use of the minimum quantity of ammunition for combined handgun and shoulder-fired weapons necessary to demonstrate the ability to effectively implement the licensee's protective strategy

For sites that use ROWS, the training and qualification plan shall identify the incorporation of ROWS within the tactical qualification course for ROWS operators as applicable.

14. Section VI.G, "Weapons, Personal Equipment, and Maintenance," of Appendix B to 10 CFR Part 73

Guidelines

The training and qualification plan should describe the methodology to be used to ensure that armed personnel are provided with weapons that are capable of performing the function stated in the security plans, licensee protective strategy, and implementing procedures. The training and qualification plan should include a description of the firearm specifications and specific ammunition delivery mechanism (e.g., magazine-fed, belt-fed, drum-fed, etc.), including the minimum number of rounds that are required to be carried by armed personnel for each type of firearm employed at the site.

The training and qualification plan shall confirm that specifications for each type of firearm used at the facility are consistent with the requirements stated in Appendix B to 10 CFR Part 73.

The training and qualification plan shall confirm that the firearms and ammunition employed at the site meet the minimum firearms and ammunition specifications (e.g., caliber, muzzle velocity, and muzzle energy) of Appendix B to 10 CFR Part 73.

For sites that use ROWS, the training and qualification plan shall confirm that the specific firearm used in the ROWS meets the minimum firearms and ammunition specifications of Appendix B to 10 CFR Part 73 and should include a description of the firearm specifications and specific ammunition delivery mechanism (e.g., magazine-fed,

belt-fed, drum-fed, etc.), including the minimum number of rounds that are available for use by the firearm used in the ROWS deployed at the site.

The training and qualification plan shall confirm that each individual is equipped with or has ready access to all personal equipment or devices required to (1) perform assigned duties and responsibilities in accordance with implementing procedures and (2) ensure the effective implementation of the Commission-approved security plans and the licensee protective strategy.

The training and qualification plan shall confirm that (at a minimum) the licensee maintains at all times the minimum number of armed security personnel required to effectively implement the Commission-approved safeguards contingency plan, site protective strategy, and site implementing procedures. The training and qualification plan should confirm that, as appropriate, personnel who are assigned duties and responsibilities required for implementation of the site's physical protection program are equipped with:

- a full-face gas mask
- body armor (bullet-resistant vest)
- ammunition and equipment belt
- two-way portable radios with a minimum of two channels (one operating and one emergency)

The training and qualification plan shall confirm that firearms (to include ROWS firearms, as applicable) are maintained in accordance with the requirements of Section VI.G.3 of Appendix B to 10 CFR Part 73 and the licensee's implementing procedures. The training and qualification plan should confirm that personal equipment is maintained in accordance with the licensee's implementing procedures.

The training and qualification plan shall confirm that training and qualification records are retained in accordance with 10 CFR 73.55(q), Section VI.H of Appendix B to 10 CFR Part 73, and the licensee's implementing procedures.

Safeguards Contingency Plans

In accordance with 10 CFR 73.55(c)(5), the licensee shall establish, maintain, and implement a Safeguards Contingency Plan that describes how the criteria set forth in Appendix C, section II, to this part, "Nuclear Power Plant Safeguards Contingency Plans," will be implemented. The licensee shall establish, maintain, and implement, and follow a SCP that describes how the criteria set forth in appendix C to this part, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," will be implemented." In summary the SCP descriptions should be sufficiently detailed to address the following:

Establishes defined objectives in the event of threats, thefts, or radiological sabotage relating to special nuclear material or nuclear facilities, licensees should address these criteria:

A. The background and overview of the safeguards contingency plan shall include information on:

- perceived danger
- purpose of the plan
- scope of the plan
- definitions

B. Generic Planning Base: The identification of initiation conditions, with objectives to be accomplished for each condition, and the identification of the data, criteria, procedures, and mechanisms necessary to efficiently implement decisions:

- defines the criteria for initiating and terminating a response
- identifies events that will signal the beginning or aggravation of a Safeguards contingency event
- describes the methodologies to verify the effectiveness of the processes and procedures developed to accomplish the goals and objectives for each postulated event

C. Licensee Planning Base: A description of the site-specific design and organizational structure for response, security systems, and defense-in-depth (DID) (i.e., the protective strategy):

- identifies the basis for the site-specific response strategy
- should address the placement of personnel and the use and capability of offsite resources

D. Responsibility Matrix: The identification of a mechanism that describes individuals, groups, or organizational entities responsible for each decision and action.

1. Section II, “Nuclear Power Plant Safeguards Contingency Plans,” of Appendix C to 10 CFR Part 73

The safeguards contingency plan describes how the standards and criteria set forth in Section II of Appendix C to 10 CFR Part 73 are implemented. The SCP must describe

predetermined actions, plans, and strategies designed to interdict and neutralize adversaries up to and including the DBT for radiological sabotage.

A. The acceptability of the SCP will be contingent on the applicant's or licensee's descriptions, with sufficient details, of plans of actions to achieve the goals of: (a) organizing response efforts; (b) providing predetermined and structured responses to safeguards contingencies; (c) integrating the licensee response by other entities; and (d) achieving required responses to threats up to and including the DBT for radiological sabotage.

B. The SCP will be acceptable, if the plans and actions described are adequately implemented and result in:

(i) Organizing the licensee's resources in such a way that the participants will be identified, their responsibilities specified, and their responses coordinated.

(ii) Responding in a timely manner and including personnel who are trained and qualified to respond in accordance with a documented training and qualification program. The evaluation, validation, and testing of this portion of the program shall be conducted in accordance with Appendix B to 10 CFR Part 73.

(iii) Maintaining effectiveness during the implementation of emergency plans developed under Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities," to 10 CFR Part 50.

C. The safeguards contingency plan should generally describe relationships and interactions among the safeguards contingency plan, the physical security plan, the training and qualification plan, and other nonsecurity plans as they relate to the overall physical protection program. Detailed technical information required to establish or support the technical basis for actions, described in the safeguards contingency plan but not required to understand or implement the plan, may also be captured through reference to applicable documentation, rather than by specific inclusion in the safeguards contingency plan.

D. The general description of the safeguards contingency plan should include actions and objectives to be accomplished by the security organization and explain how the stated actions and objectives are coordinated with actions that may be performed concurrently by other onsite entities, such as operations and fire protection, to avoid potential conflicts during security-related contingency events or other emergency situations that could directly or indirectly endanger the public health and safety or common defense and security.

E. The safeguards contingency plan must contain a level of information regarding contingency situations, in general, that is sufficient to ensure an understanding of duties and responsibilities necessary to effectively deal with and counter identified contingency events.

F. The safeguards contingency plan is designed and implemented to provide protection against the DBT of radiological sabotage, as described in 10 CFR 73.1, and associated adversary characteristics. RG 5.69 contains additional guidance regarding adversary characteristics associated with the DBT of radiological sabotage.

G. The safeguards contingency plan, at a minimum, shall describe the plan's background, generic planning base, licensee planning base, responsibility matrix, and implementing procedures. The licensee need not submit implementing procedures to the NRC.

2. Section II.B.1, "Background" of Appendix C to 10 CFR Part 73

Guidelines

The SCP shall describe background information in sufficient detail to address the purpose and scope of the plan, the perceived danger (a general description of the threat posed by the DBT), and any applicable definitions.

The descriptions are acceptable if the descriptions conform to the acceptable methods, approaches, or scope in Section C.1, "Background," of RG 5.54.

3. Section II.B.2, "Generic Planning Base" of Appendix C to 10 CFR Part 73

Guidelines

The descriptions are acceptable if they conform to the acceptable methods, approaches, and scope for contingency planning in Section C.2, "Generic Planning Bases," of RG 5.54. Specifically, descriptions should address in sufficient detail the generic planning bases that address these events as a minimum for contingency planning:

The descriptions of contingency planning for the events will be acceptable if the information and data are sufficiently detailed to conform to guidance provided for each event in RG 5.54.

- Event No. 1: Malevolent Threat/Use of a Vehicle
- Event No. 2: Detection of Impending Attack, Threat/Direct Armed Attack
- Event No. 3: Civil Disturbance
- Event No. 4: Protected or Vital Area Intrusion/Discovery of Breached Barrier
- Event No. 5: Fire, Explosion or Other Catastrophe
- Event No. 6: Detection of Aberrant Behavior
- Event No. 7: Security Force Strike or Unavailability of Security Force
- Event No. 8: Loss of Contact with Security Officers
- Event No. 9: Confirmed Sabotage, Tampering, Vandalism, Malicious Mischief
- Event No. 10: Bomb Threat/Explosive Device Discovered
- Event No. 11: Loss of On-Site/Off-Site Security Communications

- Event No. 12: Loss of Security System Power
- Event No. 13: Loss of Alarm Assessment Systems/IDS
- Event No. 14: Loss of Security Lighting
- Event No. 15: Loss of Security Computer
- Event No. 16: Extortion/Coercion/Hostage Threat
- Event No. 17: Waterborne Threat
- Event No. 18: Coordinated Land Vehicle Bomb Threat
- Event No. 19: Standoff Attack by a Sniper
- Event No. 20: Insider Threat
- Event No. 21: Attempted or Confirmed Cyber Attack

The safeguards contingency plan shall contain a generic planning base that identifies those events that will be used for signaling the beginning or aggravation of a safeguards contingency event, according to how they are perceived initially by licensee personnel. The generic planning base should address event initiation, such as the detection of unauthorized activities; the response to all alarms or other indications signaling a security event, such as penetration of a protected area or vital area or unauthorized barrier penetration (by vehicle or personnel); tampering; and bomb threats or other threat warnings—either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.

The generic planning base within the safeguards contingency plan shall describe specific threats or events and list the objectives to be accomplished for each event identified. The generic planning base shall also identify the data, criteria, procedures, mechanisms, and logistical support required for the evaluation and response to each event described. The licensee's site implementing procedures must address the decisions and actions of response for each event.

NUREG/CR-7145, "Nuclear Power Plant Security Assessment Guide" (ADAMS Accession No. ML13122A181) and SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual" (available at http:// prod.sandia.gov/techlib/access-control.cgi/2007/075591.pdf), contain additional guidance.

4. Section II.B.3, "Licensee Planning Base" of Appendix C to 10 CFR Part 73

Guidelines

The descriptions are acceptable if they conform to the acceptable methods, approaches, or scope for contingency planning in Section C.3, "Licensing Planning Bases," of RG 5.54. Specifically, descriptions address in sufficient detail the licensing planning bases for security response to safeguards contingency events and describe the protection of response personnel, associated onsite resources, and offsite assistance to protect against threats up to and including the DBT for radiological sabotage. The descriptions shall include these elements of the licensing planning bases:

- organization structure
- physical layout

- safeguards systems
- defense-in-depth
- response capabilities
- response requirements
- protective strategy
- law enforcement response
- policy constraint and assumptions
- administrative and logistical considerations

5. Section II.B.3.a, “Organizational Structure” of Appendix C to 10 CFR Part 73

Guidelines

The descriptions are acceptable if they conform to the acceptable methods, approaches, or scope for contingency planning in RG 5.54, Section C.3.2, “Organization Structure.” For example, the descriptions should include plans for establishing organization structure for command and control, delegation of authority, and responsibilities during a contingency event. The descriptions shall also address individual duties, descriptions of responsibility, and authority for members of the security response force during contingency events.

6. Section II.B.3.b, “Physical Layout” of Appendix C to 10 CFR Part 73

Guidelines

The safeguards contingency plan shall include a site maps, diagrams, and illustrations that depict the physical structures located on the site, including onsite independent spent fuel storage installations if applicable, and a description of the structures depicted on the map. The site maps shall also depict nearby towns, transportation routes (e.g., rail, water, and roads), pipelines, airports, hazardous material facilities, and pertinent environmental features that may affect response activities. These maps shall indicate the main and alternate routes for law enforcement or other offsite response and support agencies and locations for marshaling coordination responses.

The descriptions are acceptable if they conform to the acceptable methods, approaches, or scope for contingency planning in RG 5.54, Section C.3.3, “Physical Layout.”

For example, the descriptions shall include:

- a layout of the facility,
- a site map showing physical structures,
- descriptions of physical security systems,
- access-control points,
- site characteristics
- characteristics of nearby areas, including identification and considerations of potential manmade or natural hazards for contingency planning.

7. Section II.B.3.c, “Safeguards Systems” of Appendix C to 10 CFR Part 73

Guidelines

The descriptions are acceptable if they conform to the acceptable methods, approaches, or scope for contingency planning in RG 5.54, Section C.3.4, “Safeguards Systems”; Section C.3.5, “Defense-in-Depth”; Section C.3.6, “Response Capabilities”; C.3.7, “Response Requirements”; and Section C.3.8, “Protective Strategy.” The descriptions shall include physical security systems relied on for security response, response requirements, and areas of responsibilities for physical protection for contingency planning. For example, the descriptions provide information and data for:

A. How to respond to an event in order to protect against the DBT, as described in 10 CFR 73.1(a). The descriptions are consistent with 10 CFR Part 73, Appendix C, Section II(B)(3)(c)(v) and include the physical protection measures from the outermost facility perimeter inward to the measures that protect target sets from the DBT for radiological sabotage.

B. Physical security systems (e.g., IDS, physical barriers access controls, armaments, surveillance, communication systems) for security response.

C. The number of armed responders designated to implement the protective strategy (which shall not be fewer than 10). The number of armed security officers designated to implement the protective strategy for the site shall be documented in the safeguards contingency plan. Where ROWS are used, the safeguards contingency plan should describe the number of ROWS employed at the site and the number of ROWS operators that are required to operate these systems. The descriptions should establish whether these systems and the system operators are designated as a component of the minimum number of armed responders or designated armed security officers within the site’s protective strategy.

D. The duties and responsibilities of the security personnel used as armed responders and armed security officers to implement the site’s protective strategy within predetermined timelines. For sites that use ROWS, the duties and responsibilities of the ROWS operators should also be described in the safeguards contingency plan. This description should include operator actions and capabilities if ROWS becomes inoperable during a contingency event.

E. The written protective strategy. This written facility procedure describes the methodology to determine the existence and level of a threat, the deployment and function of the response organization (to include ROWS, if applicable) to implement the licensee’s protective strategy, and specific details about the support and capabilities of offsite law enforcement agencies.

8. Section II.B.3.d, “Law Enforcement Assistance” of Appendix C to 10 CFR Part 73

Guidelines

The descriptions are acceptable if they conform to the acceptable methods, approaches, or scope for contingency planning in RG 5.54, Section C.3.9, “Law Enforcement Response.” For example, the descriptions shall include a list of available law enforcement agencies and a general description of their response capabilities and their criteria for response, as well as a discussion of working agreements or arrangements for communicating with these agencies.

9. Section II.B.3.e., “Policy Constraints and Assumptions” of Appendix C to 10 CFR Part 73

Guidelines

The descriptions are acceptable if they conform to the acceptable methods, approaches, or scope for contingency planning in RG 5.54, Section C.3.10, “Policy Constraint and Assumption.” The safeguards contingency plan shall describe the application of State laws, local ordinances, and established policies and practices that govern the security response to incidents, which include but are not limited to:

- use of deadly force
- recall of off-duty employees
- site jurisdictional boundaries
- use of enhanced weapons, if applicable

10. Section II.B.3.f., “Administrative and Logistical Considerations” of Appendix C to 10 CFR Part 73

Guidelines

The descriptions are acceptable if they conform to acceptable methods, approaches, or scope for contingency planning in RG 5.54, Section C.3.11, “Administrative and Logistical Considerations.”

11. Section II.B.3.f, “Responsibility Matrix” of Appendix C to 10 CFR Part 73

Guidelines

The descriptions are acceptable if they conform to acceptable methods, approaches, or scope for contingency planning in RG 5.54, Section C.4, “Responsibility Matrix.” For example, the descriptions shall include the responsibility matrix and responsibility-matrix procedures, as well as the detailed identification of responsibilities and specific actions to be taken by licensee organizations and personnel in response to safeguards contingency events. The information should confirm that the predetermined actions identified in the responsibility-matrix procedures can be completed under the postulated conditions.

The descriptions of how site procedures will be established, maintained, and implemented should include matrices detailing the organization and personnel responsible for decisions and actions associated with specific responses to safeguards contingency events. Responsibility-matrix procedures shall address the contingency responses for the safeguards events outlined in the generic planning base.

12. Section II.B.5, "Implementing Procedures" of Appendix C to 10 CFR Part 73

Guidelines

The descriptions must indicate that licensees shall establish and maintain written implementing procedures that provide specific guidance and operating details identifying the actions to be taken and decisions to be made by each member of the security organization who is assigned duties and responsibilities required for the effective implementation of the security plans and the site's protective strategy.

IV. EVALUATION FINDINGS

For COL and OL reviews, the findings will also summarize the staff's evaluation of requirements and restrictions (e.g., interface requirements and site parameters), COL action items, and license conditions relevant to this SRP section. The evaluation finding at the COL and OL should be substantially equivalent to this statement (do not include any of the quotation marks, except those that start and end titles, if this statement is cut and pasted into another document):

The NRC staff reviewed the [insert plant name], which establishes the basis for licensing in its descriptions of engineered and administrative controls and management systems (i.e., **[insert "COLA" or "OL"]** Parts 1, 2, 7, 8, 9; the Security Plan (the PSP, T&QP, and SCP); and the cited **[insert cited technical reports or other documents on the docket and/or cited certified design documents where applicable]**) for the physical protection of the proposed operations of [insert plant name]. The staff concludes that:

- "The COL applicant meets the requirements of **[insert "10 CFR 52.79(a)(35)(i) and (ii)" or "10 CFR 50.34(c) through (e)"]**, which state that information submitted for a **[insert "COL" or "OL"]** must describe how the applicant will meet the requirements of 10 CFR Part 73 and provide descriptions of (i.e., the schedule and milestones for) the implementation and maintenance of the licensing basis for security.

- "The licensing bases, along with design bases for security SSCs relied on to protect **[inset plant name]** against threats up to and including the DBT, is adequately described in the COLA, which includes the Security Plan and technical reports and regulatory guidance that are incorporated by reference (i.e., FSAR Parts1, 2, 7, 8, and 10; the PSP, T&QP, and SCP; the **[insert cited technical reports or other documents on the docket and/or cited certified design documents where applicable]**).

- "The **[insert "COL" or "OL"]** applicant adequately described in the **[insert "COLA" or "OL"]**, and established the licensing basis of, how it will meet the performance and prescriptive requirements of 10 CFR Part 73, including Appendices B and C, for the licensing of a utilization facility under 10 CFR Part 52. Specifically, the **[insert "COL" or "OL"]** applicant adequately described the licensing basis that (1) integrates the design of engineered physical security systems, operational requirements, and management system for a physical protection program (as described in the **[insert "COLA" or "OL"]**) for the adequate protection of **[insert plant name]**, (2) establishes the operational requirements and management system for the implementation of the training and qualification of security personnel performing security functions, and (3) establishes the operational requirements and a management system for developing, implementing, and maintaining written plans and procedures that implement the protective strategy.

  The Security Plan (the PSP, T&QP, and SCP)include details of physical protection measures, engineered PSS, and deployment of the armed security response for safeguard contingency response. The NRC staff has determined that these plans include the necessary programmatic elements that, when effectively implemented, will provide the required high assurance as describe in 10 CFR 73.55(b)(1). (i.e., provide high assurance that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety). The burden to effectively implement these plans remains with the applicant. Effective implementation depends on the procedures and practices that the applicant develops to satisfy the programmatic elements of its PSP, T&QP, and SCP. The target-set analysis and the site's protective strategy are in facility implementing procedures which were not subject to NRC staff review as part of this COL application and are therefore subject to future NRC inspection in accordance with 10 CFR 73.55(c)(7)(iv) and 10 CFR Part 73, Appendix C, Section II.B.5(iii).

  As required by Section 3 of the applicant's PSP, a performance-evaluation program will be implemented that periodically tests and evaluates the effectiveness of the overall protective strategy. This program requires that deficiencies be corrected. In addition, NRC inspectors will conduct periodic force-on-force exercises that will test the effectiveness of the applicant's protective strategy. Based on the results of the applicant's own testing and evaluation, the NRC's baseline inspections, and force-on-force exercises, enhancements to the applicant's PSP, T&QP, and SCP may be required to ensure that the overall protective strategy can be effectively implemented. As such, staff approval of the applicant's PSP, T&QP, and SCP is limited to the programmatic elements necessary to provide the required high assurance as stated above. Should deficiencies be identified with the programmatic elements of these plans as a result of the periodic applicant- or NRC-conducted drills or exercises that test the effectiveness of the overall protective strategy, the applicant shall correct the plans to address these deficiencies in a timely manner and shall notify the NRC of these plan changes in accordance with the

requirements of 10 CFR 50.54(p) or 10 CFR 50.90, "Application for amendment of license, construction permit, or early site permit."

The **[insert "COL" or "OL"]** applicant's descriptions and information in the Security Plan for the physical protection program at **[insert plant name]**, submitted on the docket, conform to acceptance criteria in NUREG-0800, Section 13.6.1, and therefore are acceptable.

The staff concludes that the licensing basis described in the **[insert "COLA" or "OL"]**, if the **[insert plant name]** facility is adequately designed, constructed, installed, maintained, and implemented as described, satisfies the requirement for achieving the objective of high assurance that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety.

The staff also concludes that, with respect to the physical protection of the proposed operations of **[insert plant name],** the **[insert "COL" or "OL"]** applicant meets the applicable standards and requirements of the Atomic Energy Act of 1954 and NRC regulations for security, and that reasonable assurance exists that the facility will be constructed and will operate in conformity with the license, the provisions of the Atomic Energy Act of 1954, and NRC regulations. The staff further concludes that the issuance of the license will not be inimical to the common defense and security or to the health and safety of the public.

The COL or OL applicant's security-plan information is withheld from public disclosure in accordance with the provisions of 10 CFR 73.21.

V. IMPLEMENTATION

The staff may use this SRP section in performing safety evaluations of license and amendment applications submitted under 10 CFR Part 50 or 10 CFR Part 52. Except when the applicant proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the staff will use the method described here to evaluate conformance to Commission regulations.

VI. REFERENCES

1. U.S. Nuclear Regulatory Commission, "Combined License Application for Nuclear Power Plants (LWR Edition)," Regulatory Guide 1.206, available at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/rg/01-206/.

2. U.S. Nuclear Regulatory Commission, "Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas," Regulatory Guide 5.7, ADAMS Accession No. ML003739976.

3. U.S. Nuclear Regulatory Commission, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials," Regulatory Guide 5.12, ADAMS Accession No. ML003740035.

4. U.S. Nuclear Regulatory Commission, “Perimeter Intrusion Alarm Systems,” Regulatory Guide 5.44, ADAMS Accession No. ML003739217.

5. U.S. Nuclear Regulatory Commission, “Vital Area Access Controls, Protection of Physical Security Equipment, and Key and Lock Controls,” Regulatory Guide 5.65, ADAMS Accession No. ML003739336.

6. U.S. Nuclear Regulatory Commission, “Protection Against Malevolent Use of Vehicles at Nuclear Power Plants,” Regulatory Guide 5.68, ADAMS Accession No. ML003739379.

7. U.S. Nuclear Regulatory Commission, “Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements” (as it relates to the design of physical security systems), Regulatory Guide 5.69, ADAMS Accession No. ML13151A355, not publicly available.

8. U.S. Nuclear Regulatory Commission, “Physical Protection Programs at Nuclear Power Reactors,” Regulatory Guide 5.76, ADAMS Accession No. ML13151A355.

9. U.S. Nuclear Regulatory Commission, “Insider Mitigation Program,” Regulatory Guide 5.77, ADAMS Accession No. ML13151A355, not publicly available.

10. U.S. Nuclear Regulatory Commission, “High Security Protected and Vital Area Barrier/Equipment Penetration Manual,” Regulatory Issue Summary 2003-06, not publicly available.

11. U.S. Nuclear Regulatory Commission, “Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants,” *Federal Register*, Vol. 50, No. 153, August 8, 1985, pp. 32138–32150, ADAMS Accession No. ML003711521.

12. U.S. Nuclear Regulatory Commission, “Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees,” NUREG-1959, March 2011, ADAMS Accession No. ML11112A009.

13. U.S. Nuclear Regulatory Commission, “Access Control Systems: Technical Information for NRC Licensees,” NUREG-1964, April 2011, ADAMS Accession No. ML11115A078.

14. U.S. Nuclear Regulatory Commission, “Vehicle Barriers: Emphasis on Natural Features,” NUREG/CR-4250, July 1985.

15. U.S. Nuclear Regulatory Commission, “Entry/Exit Control Components for Physical Protection Systems,” NUREG/CR-5899, November 1992.

16. U.S. Nuclear Regulatory Commission, “Protection Against Malevolent Use of Vehicles at Nuclear Power Plants: Vehicle Barrier System Siting Guidance for Blast Protection,” NUREG/CR-6190, Vols. 1 and 2, Rev. 1, December 1994; the two volumes are available

at www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA325232 and www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA326506 respectively.

17. U.S. Nuclear Regulatory Commission, "Nuclear Power Plant Security Assessment Guide," NUREG/CR-7145, April 2013, ADAMS Accession No. ML13122A181.

18. U.S. Department of Energy, Sandia National Laboratories, "Technology Transfer Manuals," not publicly available:

- SAND99-2388, "Interior Intrusion Detection"
- SAND99-2389, "Video Assessment"
- SAND99-2390, "Alarm Communication"
- SAND99-2391, "Exterior Intrusion Detection"
- SAND99-2392, "Protecting Secure Communications"
- SAND99-2486, "Explosives Protection"
- SAND2000-2142, "Entry Control and Contraband Detection Systems"
- SAND2001-2168, "Access Delay Technology," Volume 1

19. U.S. Department of Defense, "Structures to Resist the Effects of Accidental Explosions"; United Facilities Criteria (UFC) 3-340-02, December 2008, available at http://www.wbdg.org/ccb/DOD/UFC/ufc_3_340_02.pdf.

20. U.S. Department of Justice, National Institute of Justice, "Ballistic Resistant Protective Materials," NIJ Standard 0108.01, September 1985, available at http://www.ncjrs.gov/pdffiles1/nij/099859.pdf.

21. Underwriters Laboratories, Inc., "Standard for Bullet-Resisting Equipment," UL 752, September 2005.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the Standard Review Plan are covered by the requirements of 10 CFR Part 50 and 10 CFR Part 52, and were approved by the Office of Management and Budget, approval numbers 3150-0011 and 3150-0151.

PUBLIC PROTECTION NOTIFICATION

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number
.