U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

13.6.2 PHYSICAL SECURITY — REVIEW OF PHYSICAL SECURITY SYSTEM DESIGNS – STANDARD DESIGN CERTIFICATION AND OPERATING REACTOR LICENSING APPLICATIONS

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of physical security

Secondary - Licensing organization and cognizant review organization per the Standard Review Plan (SRP) sections identified in the 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 physical security review of designs of physical security systems contained in a design certification (DC) or a combined license (COL) application submitted in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" or an operating license (OL) application submitted in accordance with 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities." The staff review guidance is limited to the design of engineered physical security systems, hardware, and features (hereafter referred to as "physical security systems") that are within the scope of a proposed standard design. The scope of the review includes physical security system design descriptions, including facility and structure physical arrangement drawings; plan and sectional views of structures, systems, and components (SSCs); systems schematics and diagrams; functional diagrams; system single line diagrams; tables; control logic schematics; calculations; and analyses establishing the design basis of the physical security systems described in the FSAR, also referred to as the design control document (DCD) for a DC application, or in the FSAR and security plans for a COL application

Revision 2 –June 2015

and an OL application. The review also includes topical or technical reports incorporated by reference into the DC application. The purpose of the review is to determine whether the design of the physical security systems are in accordance with the performance and prescriptive regulatory requirements of 10 CFR Part 73, "Physical Protection of Plants and Materials," that apply to a nuclear power plant.

In accordance with the requirements of 10 CFR 52.47, "Content of Applications; Technical Information," the information submitted for a DC must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the U.S. Nuclear Regulatory Commission (NRC) and procurement specifications and construction and installation specifications by an applicant. The design of physical security systems and hardware, and the associated inspections, tests, analyses, and acceptance criteria (ITAAC), are within the scope of the DC and must be included in the application submitted for certification.

The regulatory basis for the staff's review of physical security systems is established by the requirements of 10 CFR 52.48, "Standards for Review of Applications," which require the staff to review applications for compliance with the standards set out in 10 CFR Part 73. The staff's review is limited to the design of physical security systems within the nuclear power plant, and structures and plant areas included in the scope of a DC. Only the performance and prescriptive regulatory requirements of 10 CFR Part 73 addressing design of physical security systems for a nuclear power reactor (i.e., a utilization facility under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants") are applicable. The staff also reviews the designs of structures, systems, components, and features that are relied on to perform physical security response functions. The design information must be sufficiently detailed to establish design bases capturing intended security functions to support completion of detailed designs of physical security systems for procurement, construction and installation, and to support the required inspections, tests, and analyses (ITA), used to establish that the acceptance criteria are met, as required by 10 CFR 52.103(g).

This SRP section provides staff guidance for the review of physical security system designs meeting the regulatory requirements in 10 CFR Part 73. Therefore the applicability of guidance in this SRP addressing the specific requirements in 10 CFR Part 73 are not limited only to the review of a DC application under the provisions of Subpart B to 10 CFR Part 52, but are also applicable in the review of those portions of a COL or an OL application (under the provisions of Subpart C of 10 CFR Part 52 or 10 CFR Part 50, respectively) that relate to physical security system design.

The NRC staff will:

1. Review the design of physical security systems intended to meet the performance and prescriptive requirements of 10 CFR Part 73, as well as conform to guidance provided in NRC Regulatory Guide (RG) 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)." The review addresses the interface between the standard design and the COL application by examining any COL information items necessary to address the designs of physical security systems and physical security (PS)-ITAAC as site-specific or COL information, that are outside the scope of the standard design certification.

2. Identify interfaces to ensure that the review (i.e., as secondary reviewer) includes information addressed under other sections of NUREG 0800 for the design descriptions

for plant SSCs that are credited to perform security functions (e.g., physical barrier, plant lighting, communications, primary and backup electrical power, uninterruptable power supply (UPS) and any early site permit (ESP) design parameters that must be addressed in the design of physical security systems.

Scope of the Technical Review for Physical Security

1. As stated in SECY-11-0024, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," dated February 18, 2011, the level of review for a particular SSC is derived from both the SSC's safety importance (i.e., safety-related or nonsafety-related) and risk significance. The introduction to NUREG-0800, Part II, describes the licensing review philosophy and framework the NRC staff applies for new reactor DC and COL applications under 10 CFR Part 52. 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 appropriate level determined 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 (i.e., conditional risk with a probability equal to one). 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 the design basis threat (DBT) for radiological sabotage.

2. At a minimum, the DC application must provide sufficiently detailed design information to permit the preparation of acceptance and inspection requirements by the NRC and procurement, construction and installation specifications by an applicant for the physical security systems within the scope of the design. This information typically includes the design of physical protection systems providing detection, assessment, communications, delay and response functions, which are relied on to protect against the DBT of radiological sabotage, and is subject to established prescriptive design requirements of 10 CFR Part 73. The review of design descriptions for physical security systems should include SSCs relied on to protect against insider threats and implementing interior security response within the nuclear island and structures. The design descriptions should include the physical security systems for providing delay of adversaries, the protection of security responders (e.g., mall gates, vault doors, grenade nets, protected fighting positions.), and engineered non-portable lethal and non-lethal weapon systems within the nuclear island and structures. The staff will review the design descriptions submitted to determine how the proposed design of physical security systems meet the applicable performance and prescriptive requirements for physical security systems in 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage."

3. Table 13.6.2.1, "Design of Physical Security Systems within the Nuclear Island and Structures," see below, identifies the performance and prescriptive design requirements that should be addressed for the nuclear island and structures in the scope of a DC application, in accordance with the requirements of 10 CFR 52.47. The descriptions for the design of physical security systems that are within the nuclear island and structures should include the SSCs for interior detection/assessment, communication, delay, security response, and access control relied on to protect against the DBT, including insider threats. However, applicants for certification of a standard design or applicants for a COL may choose different methods or approaches for the design of a physical

protection system. The reviewer should apply the following criteria to determine if design descriptions of physical security systems may be omitted from the scope of the application:

(a) Physical security systems or functions will not be located within the nuclear island or structures, or

(b) Physical security systems will not be integral to the construction of the nuclear island and structures (e.g., independent of building structure, portable, etc.).

Based on the above criteria, hereinafter referred to as criterion 3(a) or criterion 3(b), the DC applicant need not address the design elements and associated description in Table 13.6.2.1, as noted. The two criteria are based on how, what, and where the design of physical security systems are provided to meet prescriptive requirements. The descriptions for the scope of design for physical security should clearly specify the design elements that are outside the scope of the standard design, and indicate clearly that the COL applicant referencing the DC will complete and describe the remaining designs for physical security systems for meeting performance and prescriptive regulatory requirements. In some instances, a COL applicant may be allowed to use an administrative measure (e.g., observation by security personnel) in lieu of design feature. Each matter subject to one of the above criteria should be described in a COL information item, but is not necessary if regulations explicitly require submission of information or performance of actions being considered for a COL information item. A COL applicant is required to address the regulations regardless of whether a COL information item is identified in a certified design. As such, a DC applicant may voluntary identify design certain aspects that a COL should provide in design information, but it is not necessary to establish a COL information item.

Table 13.6.2.1: Design of Physical Security Systems within the Nuclear Island and Structures

Design Element No.	Design Descriptions	Requirement
1.	Physical security systems providing the capabilities to detect, assess, interdict, and neutralize threats up to and including the DBT and provide for defense-in-depth (DID) through the integration of systems, technologies, and equipment – as it relates to the design of physical security systems for interior detection, assessment, access control, and security response. Note: Descriptions needed not be included if criterion 3(a) or 3(b), as stated above, applies.	10 CFR 73.55(b)(3)(i) and 10 CFR 73.55(b)(3)(ii)
2.	Specific type, function, and placement of physical barriers needed to satisfy the physical protection program design requirement of 10 CFR 73.55(b) and to satisfy 10 CFR 73.2, “Definitions.”	10 CFR 73.55(e) 10 CFR 73.2 (physical barrier)
3.	Physical barriers to control (or deny) access into plant areas to satisfy the physical protection program design requirements of 10 CFR 73.55(b).	10 CFR 73.55(e)(1)(i)

Design Element No.	Design Descriptions	Requirement
4.	Physical barrier systems facilitating interior security response for DID protection against the DBT of radiological sabotage. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(e)(3)(i)(A)
5.	Physical barriers providing deterrence, delay, or support of access control.	10 CFR 73.55(e)(3)(ii)
6.	Physical security systems for securing and monitoring of openings in any barrier system to prevent exploitation of the opening.	10 CFR 73.55(e)(4)
7.	Bullet-resisting physical barriers for the reactor control room, the central alarm station, including design for bullet resisting of openings or penetrations. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(e)(5) 10 CFR 73.2 (bullet-resisting)
8.	List vital equipment to demonstrate that all vital equipment are within designated vital areas, and identify physical security systems credited as physical barriers for access to vital equipment within the nuclear island and structures.	10 CFR 73.55(e)(9)(i) 10 CFR 73.2 (vital area and vital equipment)
9.	Intrusion detection equipment and locking devices allow for rapid egress during an emergency and provide entry controls for vital areas, including locking and alarming of all unoccupied vital areas.	10 CFR 73.55(e)(9)(ii) 10 CFR 73.55(e)(9)(iii) 10 CFR 73.2 (intrusion alarm)
10.	Identify the locations of the reactor control room, spent fuel pool, central alarm station (CAS), secondary alarm station (SAS), secondary power supply systems for alarm annunciation equipment secondary power supply system for non-portable communications equipment and designated vital area barriers. Note: Descriptions need not be included if criterion 3(a) or 3(b) criterion is applicable.	10 CFR 73.55(e)(9)(v) 10 CFR 73.55(e)(9)(vi)
11.	Identify locations, and technical basis, for minimum safe standoff distances for the structural construction of the nuclear island and structures to withstand DBT of radiological sabotage land vehicle bombs.	10 CFR 73.55(e)(10) (i)(A) and 10 CFR 73.1(a)(1)(E)(iii)
12.	Identify locations, and technical basis, for minimum safe standoff distances for the structural construction of the nuclear island and structures to withstand DBT of radiological sabotage waterborne vehicle bomb.	10 CFR 73.55(e)(10)(ii) (A) and 10 CFR 73.1(a)(1)(E)(iv)

Design Element No.	Design Descriptions	Requirement
13.	Locations of vital area access portals outside of, or concurrent with, the physical barrier system.	10 CFR 73.55(g)(1)(i)(A)
14.	Access portals with locking devices, intrusion detection equipment, and surveillance equipment to achieve the intended function.	10 CFR 73.55(g)(1)(i)(B)
15.	Interior detection and assessment systems satisfying the design requirement of 10 CFR 73.55(b) and provide, at all times, the capability to detect and assess unauthorized persons and facilitate interior security response for effective implementation of a protective strategy. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(1)
16.	Interior intrusion detection equipment annunciates, and video assessment displays concurrently, in at least two onsite alarm stations. Design of intrusion detection systems include capabilities for: visual and audible annunciation of alarms; visual display of the detected activity for assessment; annunciation of alarm types and locations; tamper indications and self-checking of transmission line; automatic indication of system or component failure, backup power supply; and initiations of security response. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(2) 10 CFR 73.55(i)(3)(i) 10 CFR 73.55(i)(3)(ii) 10 CFR 73.55(i)(3)(iii) 10 CFR 73.55(i)(3)(iv) 10 CFR 73.55(i)(3)(v) 10 CFR 73.55(i)(3)(vi)
17.	Protection of alarm stations from being disabled by a single act in accordance with the DBT (i.e., to ensure survivability of at least one alarm station from such a single act). Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(4)(i)
18.	Location of the CAS inside the protected area, and the interior of the CAS must not be visible from the perimeter of the protected area. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(4)(ii)(A)

Design Element No.	Design Descriptions	Requirement
19.	Alarm station operator 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. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(4)(ii)(F)
20.	CAS and SAS are equal and redundant, such that all functions can be performed in both alarm stations. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(4)(iii)
21.	Interior surveillance systems providing capabilities for surveillance, observation, and monitoring to satisfy the design requirements of 10 CFR 75.55(b). Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(5)(i)
22.	Physical barriers and interior intrusion detection for monitoring are provided for unattended openings that intersect a security boundary to detect exploitation. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(5)(iii)
23.	Specifications for the illumination for satisfying the design requirement of 10 CFR 73.55(b) and implementing security response. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(i)(6)(i)
24.	Systems providing continuous communications with onsite and offsite resources; communications capabilities terminate in both alarm stations; radio or microwave transmitted two-way voice communication, conventional telephone; a system for communication with reactor control room; and independent power sources for non-portable communication equipment. Note: Descriptions need not be included if criterion 3(a) or 3(b) is applicable.	10 CFR 73.55(j)(1) 10 CFR 73.55(j)(4) 10 CRR 73.55(j)(4)(i) 10 CFR 73.55(j)(4)(ii) 10 CFR 73.55(j)(5) 10 CFR 73.55(j)(6)

4. The design of physical security systems within the scope of the standard design may include plant areas beyond the nuclear island and structures, as determined by the applicant. However, the scope should be clearly defined in Tier 1 and Tier 2 (FSAR) of the DC application. COL applicants who reference the certified design must describe

how the design meets regulatory requirements for physical security systems not within the scope of the DC. The certified design should clearly describe design of systems outside the scope of the DC. The staff's DC review does not include any physical security systems not included within the scope of the DC.

5. When the scope of the DC includes plant areas beyond the nuclear island and structures, as defined by the DC applicant, the staff will review the descriptions of designs and specifications for physical security systems included within the scope based on the performance and prescriptive requirements of 10 CFR 73.55, which are summarized in Appendix A, Table 13.6.2.2, "Designs of Physical Protection Systems for Plant Areas beyond the Nuclear Island and Structures," of this SRP Section.

6. The information contained in Appendix A to this SRP may be incorporated into future updates to SRP Section 13.6.1, "Physical Security - Combined License and Operating Reactors," with appropriate review interfaces for applying the guidance provided within this SRP until such an update is completed, the guidance found in this SRP section, including Table 13.6.2.2, will serve as guidance for the review of the design of physical security systems that may be addressed in a COL application.

7. The descriptions of details for the design of physical security systems, including drawings, diagrams, and figures in the license application, must be in accordance with requirements of 10 CFR 73.21, Protection of Safeguards Information: Performance Requirements, and 10 CFR 73.22, Protection of Safeguards Information: Specific Requirements for protection of safeguards information.

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

The DC application review must include 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 - ITAAC," to determine that the PS-ITAAC, including ITAAC abstracts and the proposed ITAAC verification program (i.e., management systems) are identified and addressed appropriately within the DC application. The interface with SRP 14.3.12 ensures that the design bases and the descriptions of design and specifications of physical security systems found in Tier 2 of the DC application support the Tier 1 information in the DC application that identifies PS-ITAAC, the proposed ITA, and the acceptance criteria that must be verified for a finding under 10 CFR 52.103(g) for physical security. The review and documentation of the evaluation of PS-ITAAC are not within the scope of review described in SRP Section 13.6.2.

COL Information Items, Certification Requirements, and Restrictions:

The DC application review will include COL information items, requirements, and restrictions (e.g., interface requirements and site parameters, which will be compared to the actual site characteristics established for an ESP or COL). In addition, consistent with 10 CFR 52.83, a COL applicant may rely upon a standard design falling within site design parameters established in an ESP. A COL information item may not be necessary if regulations explicitly require submission of information or performance of actions being considered for a COL information item (e.g., submission of security plans describing how 10 CFR Part 73 requirements will be met).

Should a DC applicant propose that a COL applicant address the specific design descriptions for an item identified in Table 13.6.2.1 that is within the nuclear island and structures, with reasonable justification, a COL information item should be established to identify and ensure that the specific design descriptions meeting the prescriptive requirements are addressed by a COL applicant that references the certified design. The COL applicant must address the COL information items identified in the certified design and satisfactorily describe how it will meet all applicable regulatory requirements. Additionally, a COL applicant must address the applicable interface requirements, and, if the COL application references an ESP, the COL application must satisfy the site design parameters and any other restrictions established in the ESP or justify a variance from the ESP. In any event, the COL applicant must show that the actual site characteristics fall within the site design parameters postulated in the standard design, modify the design (depart from the DCD) to accommodate the site characteristics, or reanalyze site characteristics to show that the design is acceptable at the site. This last possibility may involve the COL applicant justifying a variance from the site characteristics established in the ESP.

Review Interfaces

Other SRP sections interface with this section as follows:

1. The design descriptions and information related to the design of plant SSCs credited for performing security functions are found in Tier 1 and Tier 2 (FSAR) of the DC application. Review interfaces may be required based on the applicant's approach to the design of engineered systems that perform security functions. Examples include plant lighting systems that may perform 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.

2. The staff that has primary or lead review responsibilities, as indicated in the applicable SRP sections, will review the adequacy of the design of engineered systems. The secondary reviewers provide assurance that the interfaces are addressed when the engineered SSCs are provided to meet multiple functions (i.e., safety, security, and environmental protection).

3. The physical security review should include and confirm how the proposed designs and specifications meet the applicable physical security performance and prescriptive regulatory requirements. In these review interfaces, the security technical reviewer would be secondary to the lead reviewer to ensure that the security functions are met by the proposed designs.

4. The following topical or subject areas establish 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, "Electrical Power—Introduction"

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

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

F. NUREG-0800, SRP 9.5.2, “Communications Systems”

G. NUREG-0800, SRP 9.5.3, “Lighting Systems”

H. NUREG-0800, SRP 13.6.1, “Physical Security—Combined License and Operating Reactors”

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

The referenced 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 50.34, “Contents of applications; technical information,” as it relates to the need for an applicant to describe how they will meet the requirements of 10 CFR Part 73.

2. 10 CFR Part 52, Subpart B, “Standard Design Certifications,” as it relates to certification requirements for a standard design.

3. 10 CFR 73.2, “Definitions,” as it relates to physical security systems (e.g., bullet-resisting, physical barriers, intrusion alarm, lock, protected area, vital area, vital equipment, isolation zone).

4. 10 CFR 73.55(b), as it relates to the protection against the DBT of radiological sabotage; the design and capability of physical security systems to detect, assess, interdict, and neutralize the DBT of radiological sabotage; the defense-in-depth protection criteria through the integration of systems and technologies; and the requirement to provide high assurance that activities involving special nuclear material (SNM) are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

5. 10 CFR 73.55(e), as it relates to the design of physical security systems to be procured, constructed, and installed as physical barriers; identifying and analyzing the specific use, type, function, and placement of physical barriers relied upon or credited to control or deny access; meeting the performance requirements of 10 CFR 73.55(b) and meeting applicable design criteria in 10 CFR 73.55(e)(1) through 10 CFR 73.55(e)(10).

6. 10 CFR 73.55(g), as it relates to the design of physical security systems to be procured, constructed, and installed as access controls, to control personnel, vehicle, and material access, at each access control point, in accordance with the requirements of 10 CFR 73.55(b) to protect against the DBT of radiological sabotage and the applicable design criteria in 10 CFR 73.55(g)(1).

7. 10 CFR 73.55(h), as it relates to the design of physical security systems to be procured, constructed, and installed as search equipment to detect, deter, and prevent introduction of firearms, explosives, incendiary devices, or other items at access control portals, and video surveillance systems for monitoring by individuals initiating response at vehicle

access control points and applicable design criteria in 10 CFR 75.55(h)(2) and 10 CFR 73.55(h)(3).

8. 10 CFR 73.55(i), as it relates to the design of physical security systems to be procured, constructed, and installed as intrusion detection and assessment systems for meeting the performance requirements of 10 CFR 73.55(b) and meeting the applicable design criteria in 10 CFR 73.55(i)(1) through 10 CFR 73.55(i)(6).

9. 10 CFR 73.55(j), as it relates to the design of physical security systems to be procured, constructed, and installed to provide continuous communication capabilities for meeting the applicable design criteria in 10 CFR 73.55(j)(1) through 10 CFR 73.55(j)(6).

10. 10 CFR 52.47(b)(1), which requires a DC application to contain the proposed ITAAC necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the DC is built and will operate in accordance with the DC, the provisions of the Atomic Energy Act of 1954, as amended (the Act), and NRC regulations.

11. 10 CFR 52.80(a), which requires that a COL application contain the proposed inspections, tests, and analyses, including those applicable to emergency planning, which the licensee shall perform, and the acceptance criteria necessary and sufficient to provide reasonable assurance that if the inspections, tests, and analyses are performed and the acceptance criteria are met, the facility has been constructed and will operate in conformance with the COL, the provisions of the Act, and NRC regulations. The certified design provides the standard 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.

SRP Acceptance Criteria

The list below provides specific SRP acceptance 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 with the SRP is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria, and to evaluate how the proposed alternatives to the SRP acceptance criteria provide acceptable methods of compliance with NRC regulations.

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. RG 1.206, "Combined License Application for Nuclear Power Plants (LWR) Edition," U.S. Nuclear Regulatory Commission, Washington, DC.

2. RG 5.7, "Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas," U.S. Nuclear Regulatory Commission, Washington, DC.

3. RG 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials," U.S. Nuclear Regulatory Commission, Washington, DC.

4. RG 5.44, “Perimeter Intrusion Alarm Systems,” U.S. Nuclear Regulatory Commission, Washington, DC.

5. RG 5.65, “Vital Area Access Controls, Protection of Physical Security Equipment, and Key and Lock Controls,” U.S. Nuclear Regulatory Commission, Washington, DC.

6. RG 5.68, “Protection against Malevolent Use of Vehicles at Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, Washington, DC.

7. RG 5.69, “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, U.S. Nuclear Regulatory Commission, Washington, DC.

8. RG 5.76, “Physical Protection Programs at Nuclear Power Reactors,” U.S. Nuclear Regulatory Commission, Washington, DC.

9. RG 5.77, “Insider Mitigation Program,” U.S. Nuclear Regulatory Commission, Washington, DC.

10. Regulatory Issue Summary 2003-06, “High Security Protected and Vital Area Barrier/Equipment Penetration Manual,” U.S. Nuclear Regulatory Commission, Washington, DC.

11. NUREG-1964, “Access Control Systems: Technical Information for NRC Licensees,” U.S. Nuclear Regulatory Commission, Washington, DC.

12. NUREG-1959, “Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees,” U.S. Nuclear Regulatory Commission, Washington, DC.

13. NUREG/CR-6190, “Protection against Malevolent Use of Vehicles at Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, DC.

14. NUREG/CR-4250, “Vehicle Barriers: Emphasis on Natural Features,” U.S. Nuclear Regulatory Commission, Washington, DC.

15. NUREG/CR-5899, “Entry/Exit Control Components for Physical Protection System,” U.S. Nuclear Regulatory Commission, Washington, DC.

16. NUREG-7145, “Nuclear Power Plant Security Assessment Format and Content Guide,” U.S. Nuclear Regulatory Commission, Washington, DC.

17. Department of Energy, Sandia National Laboratories, Albuquerque, NM. “Technology Transfer Manuals”: SAND2001-2168, “Access Delay Technology, Volume 1,” SAND2000-2142, “Entry Control and Contraband Detection Systems,” SAND99-2388, “Interior Intrusion Detection,” SAND99-2389, “Video Assessment,” SAND99-2390, “Alarm Communication,” SAND99-2391, “Exterior Intrusion Detection,” SAND99-2392, “Protecting Secure Communications,” and SAND99-2486, “Explosives Protection.”

18. TN 5-1300, “Structures to Resist the Effects of Accidental Explosion,” Department of Defense, Washington, DC. (Also designated as Air Force ARF 08-22 and Navy NAVFAC P-2897.)

19. NIJ Standard 0108.01, “Ballistic Resistant Protective Materials,” National Institute of Justice, Washington, DC.

20. UL 752, “Standard for Bullet-Resisting Equipment,” Underwriters Laboratories, Inc.

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 based on sound and fundamental principles of science and human factor engineering, and that provide defensible technical bases for the proposed equivalent or alternative designs for meeting the regulatory requirements within Section II.

In general, the design of physical security systems is acceptable when the proposed design and specifications describe how the performance and prescriptive design criteria in 10 CFR 73.55 will be met. The NRC decides whether the design is acceptable based on how the design assures reliability and availability through defense-in-depth that accounts for potential system failures or malfunctions (i.e., through diversity, independence, and separation). Information pertaining to the reliability and availability of a system 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).

The design descriptions must be of sufficient detail to permit the development of detailed procurement, construction, and installation specifications by an applicant, in accordance with 10 CFR 52.48. The design descriptions are acceptable when they include sufficiently detailed information for all physical security systems within the scope of the requested DC. Acceptable design descriptions establish the design bases that support the designs, commitments, and acceptance criteria identified as PS-ITAAC and required ITA in the DC application. Also, the design descriptions for physical security systems must adequately describe how they satisfy the performance and prescriptive regulatory requirements.

The descriptions for the design of physical security systems satisfy the requirements when the design descriptions provide sufficient detail to conform to the guidance in RG 1.206 for the design scope. The acceptable level of details for design is shown in Figure 1, “Combined License Application Referencing a Certified Design,” describing the design detail and integration of design information between the DC and a combined license application (COLA), which is applicable to design information of physical security systems provided to meet applicable performance and prescriptive regulatory requirements.

The acceptance is based on meeting regulatory requirements in 10 CFR Part 73, and conforming to applicable and associated acceptance criteria for the design of the specific physical security system. In most cases, design 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 design of a system 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 52.47(a)(9). However, when the regulatory requirement is sufficiently prescriptive as to how it must be met (e.g., explicit configuration, specific times or quantities of weight, specific dimensions, exact type of material for construction), confirmatory statements or restatements of regulatory requirements may be sufficient to satisfy regulatory requirements.

The design descriptions must provide a sufficient level of detail on the proposed physical security systems within the standard design for the Commission to determine that all applicable regulatory requirements will be met. The applicant must also describe in detail how the physical

security systems will be designed, constructed, and installed to meet intended security functions and demonstrate that these systems and structures can be verified through ITA, including construction and installation verification acceptance testing.

The information below provides the specific SRP acceptance criteria for the design of security systems. The acceptance criteria are established based on regulatory requirements and are listed in the order that they appear in 10 CFR 73.55. The staff should only apply the acceptance criteria below that are applicable to the design of the physical security systems within the scope of the DC (i.e., as applicable based on the design descriptions and associated requirements identified in Tables 13.6.2.1 and 13.6.2.2):

1. 10 CFR 73.55(b)(3)(i) is satisfied when the applicant adequately describes how the design of physical security systems provides the capabilities to detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage. To meet the performance regulatory requirements, the applicant determines and proposes how it will provide or design a physical protection system (i.e., detection, assessment, communications, 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 protections systems, is satisfied when design descriptions include how physical security systems will be designed to address each element of a physical protection system for capability to detect, assess, communicate, and respond (interdict and neutralize). It includes the design and specifications addressing the reliability and availability of physical security systems that are providing or are relied on by administrative controls (i.e., people and procedures) for meeting high assurance of detection, assessment, interdiction, and neutralization. Therefore, the design descriptions should address each element of a physical protection system and must meet the requirements of 10 CFR 73.55(b)(3)(i) and (b)(3)(ii), as they relate to the design of physical security systems.

   At a minimum, applicants should address the following to satisfy the requirements of 10 CFR 73.55(b)(3)(i) and (b)(3)(ii) as they relate to design of physical security systems. The information submitted must be sufficient for completing detailed design for procurement, construction, and installation of physical security systems 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 UPS; (6) lighting specifications required for detection and assessment; (7) systems monitoring and human interfaces; and (8) technical basis for and the specifications of the DBT characteristics that are protected.

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 SSCs and their locations and interfaces; (4) protecting communication signals; (5) electrical power sources addressing primary power, secondary power, and UPS; (6) redundancy for protection against DBT characteristics affecting availability of security communications; and (7) technical basis for and the specifications of DBT characteristics protected.

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 SSCs and their interfaces; (4) electrical power sources addressing primary power, secondary power, and UPS 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) technical basis and specifications of DBT characteristics protected.

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 SSCs 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 UPS 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

UPS; (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:* 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 reasonable or 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. The NRC's philosophy applies to the designs of physical protection systems, which integrate engineered controls and administrative controls, to provide a high assurance of protection against the DBT for radiological sabotage.

2. 10 CFR 73.55(e): As it relates to the design of physical barrier systems, their uses, types, functions, and placement, to satisfy the capabilities for control and delay of access into the plant areas. The design descriptions should provide sufficient detail of how the following criteria are met:

   A. Protect against the DBT of radiological sabotage (10 CFR 73.55(e)(3)(i)(A)).

   B. Provide deterrence, delay, or support access control (10 CFR 73.55(e)(3)(ii)).

   C. Support implementation of protective strategy, response (10 CFR 73.55(e)(3)(iii)).

   D. Secure and monitor any barrier or barrier systems to prevent exploitation of the opening (10 CFR 73.55(e)(4)).

E. Provide bullet-resisting physical barriers for the reactor control room, the central alarm station, and the locations within which the last access control function for access to the protected area is performed (10 CFR 73.55(e)(5)).

F. Provide physical barriers, as needed, to satisfy the requirement of 10 CFR 73.55(b) to protect against the DBT (10 CFR 73.55(e)(6)).

G. Establish an isolation zone in an outdoor area adjacent to the protected area perimeter barrier that meets the following criteria (10 CFR 73.55(e)(7)(i)):

(i) Sufficient size to permit observation and assessment of activities on either side of the protected areas barrier (10 CFR 73.55(e)(7)(i)(A)).

(ii) Intrusion detection equipment monitoring that is capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected areas perimeter barrier (10 CFR 73.55(e)(7)(i)(B)).

(iii) Monitored with assessment equipment to satisfy the requirements of 10 CFR 73.55(i) and provide real-time and play-back/recorded video images of the detected activities before and after each alarm annunciation.

(iv) Clear of obstruction that could prevent capabilities for observation and assessment (10 CFR 73.55(e)(7)(ii)).

H. Provide protected area perimeter physical barrier systems that meet the following criteria (10 CFR 73.55(e)(8)):

(i) Limit access into the protected area (10 CFR 73.55(e)(8)(i)(A)).

(ii) Channel personnel, vehicles, and material to designated access control portals (10 CFR 73.55(e)(8))(i)(B)).

(iii) Separated from any other barriers designated as vital area physical barriers (10 CFR 73.55(e)(8)(i)(C)).

(iv) Penetration through the protected area barrier must be secured and monitored to prevent or delay, and detect the exploitation of any penetration (10 CFR 73.55(e)(8)(ii).

(v) Alarm and secure all emergency exits in the protected areas by locking devices that allow prompt egress during an emergency and satisfy the requirements for access control into the protected areas (10 CFR 73.55(e)(8)(iii)).

(vi) Where building walls or roofs comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary provided that the detection and assessment requirements of 10 CFR 73.55 are met and appropriate barriers are installed (10 CFR 73.55(e)(8)(iv)).

I. Locate vital equipment and designate vital areas for meeting the following criteria (10 CFR 73.55(e)(9)):

(i) Vital equipment is located in designated vital areas inside the protected area, and is protected by at least two physical barriers (10 CFR 73.55(e)(9)(i)).

(ii) Vital area access portals and emergency exits are protected with intrusion detection equipment and locking devices that allow rapid egress during an emergency and satisfy the vital area entry control requirements (10 CFR 73.55(e)(9)(ii)).

(iii) Access portals and emergency exits to unoccupied vital areas are locked and alarmed (10 CFR 73.55(e)(9)(iii)).

(iv) More than one vital area may be located within a single protected area (10 CFR 73.55(e)(9)(iv)); the reactor control room, spent fuel pool, central alarm station, and secondary alarm station are designated as vital areas (10 CFR 73.55(e)(9)(v)); and the secondary power supply systems for alarm annunciation equipment and nonportable communication equipment are located within the vital area (10 CFR 73.55(e)(9)(vi)).

3. 10 CFR 73.55(e)(10*)*: As it relates to the design of vehicle control measures required to protect against the DBT of radiological sabotage vehicle bomb assault. The design descriptions should provide sufficient detail of how the following criteria are met:

A. Land-based vehicle barrier system (passive and active barriers) is at a standoff distance adequate to protect personnel, equipment, and systems necessary to prevent significant core damage and spent fuel pool sabotage against the effects of the DBT of radiological sabotage land vehicle bomb assault (10 CFR 73.55(e)(10)(i)(A)).

B. A secondary power source or a means of mechanical or manual operation in the event of a power failure performs the intended function to deny unauthorized vehicle access beyond the required standoff distance (10 CFR 73.55(e)(10)(i)(B)).

C. Install train derailer, remove a section of track, or restrict access to railroad sidings where a site has rail access into the protected area (10 CFR 73.55(e)(10)(i)(D)).

D. Waterborne vehicle barrier system restricts waterway approaches, and, where possible, deploy buoys, markers or other equipment (10 CFR 73.55(e)(10)(ii)(A)).

4. *10 CFR 73.55(g)*: 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. The design descriptions provide sufficient detail of how the following criteria are met:

A. Locate access control portals outside of, or concurrent with, the physical barrier system through which it controls access (10 CFR 73.55(g)(1)(i)(A)).

B. Equip access control portals with locking devices, intrusion detection equipment, and surveillance equipment to achieve the intended function (10 CFR 73.55(g)(1)(i)(B)).

C. Provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment located at or outside the protected area (10 CFR 73.55(g)(1)(i)(C)).

D. Design access control systems to accommodate the potential need for rapid ingress and egress (10 CFR 73.55(g)(5)(i)).

5. *10 CFR 73.55(h)(3)(i)*: As it relates to the design of physical security systems that satisfy the requirements for search and control of access of individuals, vehicles, and material to protected areas. The design descriptions should provide sufficient details of how the following criteria are met:

A. Search for and detection of firearms, explosives, incendiary devices, and other items that could be used for radiological sabotage (10 CFR 73.55(h)(3)(i)),

B. Control of access for vehicles, and video surveillance along with systems for vehicle access points, and video surveillance equipment address the capability to allow for monitoring by an individual capable of initiating a response (10 CFR 73.55(h)(2)(v)).

6. *10 CFR 73.55(i)*: As it relates to design of detection and assessment systems that satisfy the requirement of 10 CFR 73.55(b) for the capability to detect and assess unauthorized access at all times and facilitate the implementation of security response. The design descriptions should provide sufficient details for how the following criteria are met:

A. Intrusion detection equipment must annunciate and video assessment equipment must display concurrently in at least two onsite alarm stations. One of the alarm stations must be designed to meet the requirements of a central alarm station (10 CFR 73.55(i)(2)).

B. Visual and audible annunciation of an alarm (10 CFR 73.55(i)(3)(i)), and annunciation must identify the type and location of the alarm (10 CFR 73.55(i)(3)(iii)).

C. Provide a visual display for assessment of the detected activity (10 CFR 73.55(i)(3)(ii)).

D. Transmission lines from alarm devices to annunciators are tamper indicating and self-checking (10 CFR 73.55(i)(3)(iv)).

E. 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 (10 CFR 73.55(i)(3)(v)).

F. Uninterruptible power supply for continued operations of intrusion detection and assessment equipment at the protected area perimeter in the event of the loss of normal power (10 CFR 73.55(i)(3)(vii)).

7. *10 CFR 73.55(i)(4)*: As it relates to design of alarm stations that satisfy the requirement of 10 CFR 73.55(b) for the capability to detect and assess unauthorized at all times, and

facilitate the implementation of security response. The design descriptions should provide sufficient details for how the following criteria will be met:

A. Both alarm stations are designed to ensure that a single act cannot disable both alarm stations and the design ensures the survivability of at least one alarm station, including the capability to perform the following functions: (1) detect and assess alarms; (2) initiate and coordinate response to an alarm; (3) summon offsite assistance; and (4) provide command and control (10 CFR 73.55(i)(4)(i)(A) through (i)(4)(i)(D)).

B. Locate the central alarm station inside the protected area and the interior of the central alarm station must not be visible from the perimeter of the protected area (10 CFR 73.55(i)(4)(ii)(A)).

C. Alarm station operator 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 (10 CFR 73.55(i)(4)(ii)(F)).

D. Both alarm stations are equal and redundant, such that all functions needed to satisfy the requirements of 10 CFR 73.55(i)(4)(iii)) are met.

8. *10 CFR 73.55(i)(5)*: As it relates to the design of physical security systems for surveillance, observation, and monitoring that satisfy the requirement of 10 CFR 73.55(b) for the capability to detect and assess unauthorized at all times, and facilitate the implementation of security response. The design descriptions should provide sufficient detail for how the following criteria will be met:

A. Video technology continuous surveillance, observation, and monitoring of the owner controlled area and ensure the integrity of physical barriers or other components and functions (10 CFR 73.55(i)(5)(ii)).

B. Physical barriers and interior intrusion detection are provided for unattended openings that intersect a security boundary to detect exploitation (10 CFR 73.55(i)(5)(iii)).

9. *10 CFR 73.55(i)(*6): As it relates to design of engineered systems for illumination that satisfy the requirement of 10 CFR 73.55(b) and facilitate detection, assessment, surveillance, and security response at all times. The design descriptions should provide sufficient detail of how the following criteria are met:

A. Illumination systems for all areas of the facility for illumination necessary to perform detection, assessment, interdiction and neutralization (10 CFR 73.55(i)(6)(i)).

B. Minimum illumination level of a 0.2 foot-candle, measured horizontally at ground level, in the isolation zones and appropriate exterior areas within the protected area (10 CFR 73.55(i)(6)(ii)).

C. Low-light technology that will be used to augment facility illumination systems (10 CFR 73.55(i)(6)(ii)).

10. *10 CFR 73.55(*j): As it relates to design of security or plant communication systems that satisfy the requirement of 10 CFR 73.55(b) for protection against the DBT of radiological sabotage and facilitate security response onsite and offsite. The design descriptions should provide sufficient detail of how the following criteria are met

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

    B. Capabilities for communication by radio or microwave transmitted two-way voice communication, either directly or through an intermediary, and conventional telephone service between the site and local law enforcement authorities, at both alarm stations (10 CFR 73.55(j)(4)(i)).

    C. A system for communication with the control room in both alarm stations (10 CFR 73.55(j)(4)(ii)).

    D. Independent power sources for nonportable communications equipment to remain operable in the event of the loss of normal power (10 CFR 73.55(j)(5)).

    E. Communication measures for site areas where communication could be interrupted or cannot be maintained (10 CFR 73.55(j)(6)).

Technical Rationale

The technical rationale for application of these acceptance criteria to the areas of review addressed by this SRP section is discussed in the following sections and paragraphs:

1. Independent of the licensing regulations and licensing approaches established in 10 CFR Part 52 (or 10 CFR Part 50); the physical protection for a nuclear power plant must meet the requirements of 10 CFR Part 73. Under Subpart B, “Standard Design Certifications,” of 10 CFR Part 52, a DC application must include performance requirements and design information sufficient to permit the NRC to prepare acceptance and inspection requirements and the applicants to prepare procurement specifications and construction and installation of physical security systems. In accordance with the requirements of 10 CFR 52.48, “Standards for Review of Applications,” the NRC will review the applications for compliance with the standards set out in 10 CFR Part 73.

2. The scope of a DC application includes the physical security systems relied on for implementing operational requirements (i.e., administrative controls) for protecting against the DBT of radiological sabotage. The referenced sections of 10 CFR Part 52 (or 10 CFR Part 50), and the associated sections of RG 1.206 (or RG 1.70 “Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” for 10 CFR Part 50), specify the scope, content, and format of the material in an application and the staff’s associated technical review. Under 10 CFR Part 52, the DC review is limited to the designs of physical security systems. The review of operational requirements and elements of physical protection programs (i.e., administrative controls and management systems) that are relied on or applied to physical security systems for establishing physical protection for nuclear material and nuclear operations of an operating reactor are reserved for a COL licensing review.

3. The acceptable level of detail for the design descriptions of physical security systems submitted with the DC application (and COL application) conforms to guidance in RG 1.206. Figure 1, "Combined License Application Referencing a Certified Design," of RG 1.206 illustrates and provides guidance for the minimum design scope described in a DC application and the remaining information needed in a COL application, and therefore is applicable to this SRP section to ensure uniform technical reviews. The staff guidance within this SRP conforms to Figure 1 in RG 1.206 for the designs of physical security systems. The acceptable descriptions of designs and specifications of physical security systems in applications submitted for DC (or COL) is a minimum FSAR level of design information to provide reasonable assurance for completion of the detailed designs for procurement, construction, and installation of physical security systems that will meet the applicable regulatory requirements of 10 CFR Part 73.

4. The COL applicant referencing a DC must provide the remaining design descriptions to complete the designs of required physical protection systems, along with the operational programs and management systems for meeting all applicable requirements in 10 CFR Part 73. The construction and installation of physical security systems are verified through the performance of required ITA and the satisfaction of the associated acceptance criteria to provide a basis for the 10 CFR 52.103(g) findings.

5. The Commission may not grant a construction permit (CP), operating license (OL), or COL unless it determines that an application meets the standards and requirements of the Act and NRC regulations. This includes notifications, if any, to other agencies and bodies. If an application for a license references a certified standard design, the certified standard design provides, in part, the design of physical security systems (i.e., the portion of the design) within the scope of the certified standard design.

6. The sections of 10 CFR Part 73 referenced in this SRP section specify the requirements for designs of physical security systems relied on or credited to implement a physical protection program 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 in this section, is required for issuance of a COL or an operating license for a nuclear power reactor pursuant to 10 CFR Part 52 or 10 CFR Part 50, respectively. The DC application, in part, describes the designs of physical security systems that will be used to establish the engineered controls provided to integrate with administrative controls for the capabilities to detect, assess, interdict, and neutralize the DBT of radiological sabotage.

7. 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.

8. The acceptability of the design of physical security systems will be based on descriptions that demonstrate (i.e., provide evidence) how the applicant's proposed standard design incorporated physical security systems or plant systems or features that meet requirements of 10 CFR Part 52 or 10 CFR 50 and 10 CFR Part 73.

III. REVIEW PROCEDURES

The generic considerations covered in the staff's review of a DC application include the following:

1. The staff bases its review on the identified SRP acceptance criteria stated in Section II of this SRP section. 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 the proposed alternative provides an acceptable method of complying with the regulations that underlie the acceptance criteria, is sufficient to meet 10 CFR 52.47(a)(9). 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 section.

2. The primary reviewer reviews the application for information (i.e., Tier 1 and Tier 2 (FSAR) and referenced technical reports) related to the design bases and design descriptions for physical security systems. The reviewer determines whether the scope of the DC application conforms to, and descriptions are provided to address, the physical security systems design descriptions and requirements identified in Table 13.6.2.1 in Section I of this SRP section. This section provides the basis for acceptance of the application for consideration of further technical review. The failure to provide, in the contents of the application, the design descriptions addressing the physical security systems conforming to Table 13.6.2.1 is a justification and technical basis for not proceeding with further technical review of a DC application.

3. The descriptions and information submitted on the docket will be reviewed to determine how the applicant's proposed designs of physical security systems satisfy the guidance in Table 13.6.2.1, which is based on the applicable performance and prescriptive regulatory requirements of 10 CFR 73.55. Table 13.6.2.1 applies to physical security systems that are within the scope of a DC application, as such systems are physically located within the nuclear island and structures or relate to the specific structural characteristics, performance, and designs of the structures (e.g., minimum standoff distance).

4. The design descriptions include drawings (plan and section views), line and block diagrams, system and component schematics, system location and configuration, specification of material and structural construction, specification on system performance, and intended security functions, at a level of detail sufficient to determine whether the SRP acceptance criteria are met. At a minimum, the level of detail of design should conform to the guidance in RG 1.206, as previously discussed, to provide reasonable assurance and adequate information for completing detailed the design of physical security systems.

5. The review of designs of physical security systems includes how the designs of these systems address defense-in-depth by means of diversity, redundancy, and separation. Where applicable, the system design margins, as previously discussed, for proposed design of physical security systems are reviewed and included as a part of the design basis for detailed design, procurement, construction, and installation.

6. For physical security systems providing the capability for detection, assessment, and response (i.e., interdiction and neutralization), the review includes how the designs of physical security systems address defense-in-depth by means of diversity, redundancy, and separation. Where applicable, the system design margins to achieve defense-in-depth, as previously discussed, for proposed design of physical security systems are reviewed and included as a part of the design basis for detailed design, procurement, construction, and installation.

The specific considerations covered in the staff's physical security review include the following:

1. Review of the proposed designs of physical security systems for how they will provide capabilities to detect, assess, interdict, and neutralize in accordance with the standards and criteria as set forth by regulatory requirements and SRP acceptance criteria in Section II. The review of specific design descriptions should follow the generic review guidance indicated above, with an emphasis on the design for defense-in-depth through diversity, redundancy, and separation to provide systems' reliability and availability to achieve high assurance of intended security functions.

2. Review of all design descriptions (text, drawings, figures, illustrations, schematics, tables, etc.) pertaining to physical security systems, including plant structures, systems, and configurations credited to provide security functions. Reviewers evaluate drawings of the nuclear island, structures, and plant areas showing locations, configurations, and installations of physical barriers and the protection of openings to determine how the proposed designs will meet regulatory requirements and conform to acceptance criteria in Section II.

3. The technical bases for determining locations of vital area barriers will be included in the review of the applicant's identification of vital equipment in accordance with the definition of 10 CFR 73.2. The list of vital equipment should include major system and subsystem descriptions, designations, and their locations. Reviewers evaluate the designated vital area barriers to confirm that the design descriptions meet regulatory requirements and conform to acceptance criteria in Section II.

4. Review of descriptions of passive and active physical barriers, including those that protect openings by locking, alarms, monitoring, and access controls. Such descriptions should clearly and concisely show how physical barrier design assures that the barrier performs its intended functions, such that it satisfies the applicable regulatory requirements and conforms to SRP acceptance criteria in Section II. References to analytical or test data should be reviewed to ensure capabilities of proposed designs and assumptions are reasonable for delay of adversaries to penetrate physical barriers. The design descriptions should also include the major systems, key subsystems and components for locking, alarms, and monitoring, and their interfaces with other physical security systems. Reviewers evaluate the proposed design for how it conforms to the definition of "physical barriers" in 10 CFR 73.2, "Definitions," and the applicable design guidance for these systems as described in RG 5.76, NUREG-1964, and NUREG-1959.

5. Review of physical barrier materials of construction, where applicable, for bullet resistance to satisfy the applicable regulatory requirements and conform to SRP acceptance criteria in Section II. The review includes the descriptions of designs and performance margins of the physical barriers, the technical basis for crediting structural walls, floors, ceilings, and protection of openings to ensure that the designs describe how they will provide the necessary minimum level of bullet resistance to protect

occupants and equipment. RG 5.76, Section 4.6.2, provides guidance on the minimum acceptable level for bullet resistance to protect against the DBT of radiological sabotage.

6. Review of the design and specification on how interior intrusion detection systems (IDS) and assessment equipment will satisfy the regulatory requirements and conform to SRP acceptance criteria in Section II. The review includes diagrams, schematics, and system specifications showing how the IDS and assessment equipment is designed and the systems specifications (e.g., types of detection technologies, intended security functions, design considerations of environmental conditions, etc.). The review should also consider whether system diagrams and schematics of the major systems and subsystems provide sufficient information for completing detailed design for procurement, construction, and installation. This includes diagrams, schematics, and specifications for the design of the IDS and system interfaces (e.g., central process units, control panels, method of alarm transmission, alarm annunciation, system cabling, entry control systems, primary and secondary power supplies, system supervision and trouble indications, system component status changes, types and locations of detection sensors, environmental protection enclosures, etc.). Reviewers evaluate the proposed design for how it conforms to appropriate guidance applicable for designs of intrusion detection systems in RG 5.44, RG 5.69, RG 5.76, NUREG-1959, U.S. Department of Energy (DOE) SAND99-2388, and SAND99-2391.

7. Review the design and specifications for how an assessment system will be provided to satisfy the regulatory requirements and conform to SRP acceptance criteria in Section II. The review should also consider whether system diagrams and schematics of the major systems and subsystems provide sufficient information for completing detailed design for procurement, construction, and installation. They include diagrams, schematics, and specifications for the design of the assessment system and system interfaces for alarm communication and display, including human factor considerations for human and machine interface for alarm display and response. Reviewers evaluate the proposed design for how it conforms to appropriate guidance applicable for assessment system design in RG 5.76, NUREG-1959, and DOE SAND99-2390.

8. Review the design and specifications for how interior and exterior surveillance, monitoring systems, and video assessment capabilities will be provided to satisfy the regulatory requirements and conform to SRP acceptance criteria in Section II. The review includes descriptions, diagrams, schematics for design, and specifications of how the surveillance, monitoring, and assessment will be accomplished. The design descriptions should include, but not are limited to: format or types of cameras, transmission and switching systems, monitoring, recording and controller systems; fields of view, real-time observation, recording and storage of video alarms, playback capabilities, data transmission line integrity, primary and secondary power supply, UPS, system supervision and indication of trouble conditions, interfaces with alarm and entry control systems, areas of coverage, camera systems, plant lighting systems, communication links, and major electronic components for detailed design, procurement, construction, and installation. Reviewers evaluate the proposed design for how it conforms to appropriate guidance applicable for the design of security assessment systems in RG 5.76, NUREG-1959, and SAND99-2389.

9. Review the designs and specifications for how security communications will be provided on the plant site and for communications with local law enforcement agencies to satisfy the regulatory requirements and conform to SRP acceptance criteria in Section II. The

review includes the description of designs and specifications for how security communications will be provided with reliability and the specific communications system functions (e.g., incident command and control, onsite security response, and offsite law enforcement assistance). The review includes diagrams, schematics, and specifications showing the system configuration and interfaces (e.g., types of communications systems, measures for anticipated disruptions and reliable coverage within plant structures, transmission integrity, major electronic components, primary and secondary power supply, UPS, systems supervision and indications of trouble conditions, defense-in-depth, etc.). The review of whether the design and configuration of plant communications systems meet security functions is coordinated with the primary reviewer (e.g., SRP 9.5.2) as described Section I of this SRP. Reviewers evaluate the proposed design for how it conforms to appropriate guidance applicable for the design of security assessment systems in RG 5.69, RG 5.76, NUREG-1959, and SAND99-2392.

10. Review the design descriptions for how the construction and locations of the central and secondary alarm stations (CAS and SAS) and security systems (controls and displays) satisfy the regulatory requirements and conform to SRP acceptance criteria in Section II. The review includes drawings, diagrams, and schematics for design, and specifications showing the design of alarm stations (e.g., systems and components, primary and secondary power, UPS, interface between the CAS and SAS, equal and redundant functions; protection against single act, etc.) and interface with other physical security systems providing security functions (e.g., IDS, assessment, communications, physical barriers for access control, designated vital equipment and vital areas, interface with supporting systems). Reviewers evaluate the proposed designs for how they conform to appropriate guidance applicable for design of the CAS and SAS in RG 5.69, RG 5.76, DOE SAND99-2168, “Access Delay Technology,” Volume 1, DOE SAND99-2388, and SAND2000-2142.

11. Review the designs and specifications for how access controls will be provided for physical control of personnel, vehicles, and material entering into the protected area and vital area to satisfy the regulatory requirements and conform to SRP acceptance criteria in Section II. The review includes diagrams, schematics, and specifications showing the designs, configurations, and specifications for access control facilities. The review includes physical security systems for personnel, vehicles, and material searches, the integration of an access control facility with protected area or vital area physical barriers, provision for IDS, assessment, surveillance, and communications, locations and configurations for defensive fighting positions, and measures for physical control of personnel, vehicles, and material access and response to threats. Reviewers evaluate the proposed designs for how they conform to appropriate guidance applicable for the design of access control facility and systems in RG 5.7, RG 5.12, RG 5.44, RG 5.65, RG 5.66, “Access Authorization Program for Nuclear Power Plants,” RG 5.68, RG 5.69, RG 5.76, RG 5.77, NUREG-1959, DOE SAND2000-2142, SAND99-2168, DOE SAND99-2388, SAND99-2391, and SAND99-2392.

12. Review the designs and specifications for how a protected area and isolation zones will be configured to provide physical barriers for delay and will provide for integration of physical security systems to achieve isolation areas for the detection, assessment, interdiction, and neutralization of DBT threats to satisfy the regulatory requirements and conform to SRP acceptance criteria in Section II. The review includes drawings, diagrams, schematics, and specifications showing the design, interfaces, and specifications for how the protected area and isolation zone will be configured (e.g.,

configuration of the isolation zone, access control facilities for personnel, vehicles, and material, locations of physical barriers, IDS, surveillance, monitoring, and assessment equipment, plant lighting systems, and defensive fighting positions, continuous perimeter designated as a protected area and isolation zones, etc.). The review of the isolation zones includes the design and specifications for the configuration of areas adjacent to the protected area barrier to allow for assessment and observation of either side of the protected area barrier, and cleared area for performing neutralization functions. Reviewers evaluate the proposed design of the IDS configuration specifically for whether the design will provide the capabilities to detect both attempted and actual penetration of the protected area barrier before the penetration is completed. The proposed designs are reviewed for conformance with guidance applicable for the design of the access control facility and systems in RG 5.12, RG 5.44, RG 5.65, RG 5.66, RG 5.68, RG 5.69, RG 5.76, RG 5.77, NUREG-1959, DOE SAND99-2168, SAND99-2391, and SAND2000-2142.

13. Review the designs and specifications for how internal and external plant lighting will provide minimum illumination sufficient for performing detection, assessment, and security response to satisfy the regulatory requirements and conform to SRP acceptance criteria in Section II. The review includes drawings and specifications of the plant lighting systems for interior and exterior plant area credited for meeting security functions. Review how the design and configurations of plant systems provide lighting capabilities to meet minimum illumination, area of coverage, capacity, and duration under normal and emergency conditions. The review of primary and secondary electrical supplies for security functions are coordinated with primary reviewers for SRP Sections 8.1, 8.3.1, 8.3.2, 9.5.3, as described in Section I of this SRP.

14. Review the designs and specifications for how physical security systems internal and external to the nuclear island and structures will interdict and neutralize or facilitate the security responders to interdict and neutralize DBT adversaries to satisfy the requirements and conform to acceptance criteria in Section II. The review includes drawings, diagrams, schematics, and specifications showing the design, interfaces, and specifications for how the physical protection systems (e.g., bullet/blast-resistant enclosures, defensive fighting positions, mall gates, grenade nets, engineered delay systems, engineered weapon systems) are provided as standard design features for implementing a security response to interdict and neutralize DBT adversaries. Reviewers evaluate whether the engineered physical security systems have the capability to remotely neutralize DBT adversaries based on criteria and procedures in this section, as applicable for subsystems and components of the remote weapon platform providing a neutralization function (e.g., trigger signal cabling, supervision and trouble conditions, control units and displays, primary and secondary power and UPS, assessment and targeting cameras, bullet-resistant barriers, etc.).

15. Review the designs and specifications for how vehicle barrier systems (passive and active) provide protection against the DBT land-based and waterborne vehicle bombs to satisfy the regulatory requirements and conform to acceptance criteria in Section II. The review includes diagrams, schematics, and specifications showing the design, interfaces, and specifications for configurations and locations of passive and active vehicle barrier systems, supporting technical analyses and required locations, and the credited performance of active vehicle barrier system (VBS). The review includes blast analysis that establishes the design basis for the minimum standoff distances necessary to protect personnel, equipment, and systems required to prevent significant core

damage, spent fuel pool sabotage, and loss of security functions. The specific structural design of the nuclear island and structures and characteristics and physical configurations that need to be maintained to maintain the validity of the minimum safe standoff distances are clearly established as the design basis for the location of the VBS. Reviewers evaluate the proposed designs for how they conform to appropriate guidance applicable for the design of VBS RG 5.69, RG 5.76, NUREG/CR-1690, NUREG/CR-4250, and DOE SAND99-2486.

Review of interfaces between a certified design and a COL application for physical security includes the following:

1. The review of the DC application, Tier 1 and Tier 2 (FSAR), includes descriptions of PS-ITAAC within the scope of the DC, in accordance with NUREG-0800, SRP Section 14.3.12. Adequate design information (e.g., intended security functions, design bases, defense-in-depth) should be provided to established design commitments, ITA, and acceptance criteria for the physical security ITAAC identified within the scope of the DC. The guidance of SRP 14.3.12 includes provisions for COL information items for the COL applicant to provide information to ensure that all PS-ITAAC are addressed and are complete, consistent with SRP Section 14.3.12, which the Commission has determined as necessary for the determination of whether a finding under 10 CFR 52.103(g) is warranted.

2. The review of the DC application, FSAR Tier 1 and Tier 2, includes the descriptions and adequacy of a COL information item with respect to designs of physical security systems that are outside the scope of the DC, along with descriptions of the physical protection program for meeting the requirements of 10 CFR 73.55 for an operating license. The security plans submitted for a COL application are required to describe how the requirements of 10 CFR Part 73 will be met. The COL information items should be established in the FSAR, and the reviewer may identify additional COL action items as appropriate and necessary. The DC FSAR should clearly identify and concisely establish COL information items that are to be addressed by a COL applicant.

For the review of a DC application, the reviewer should follow the above procedures to verify that the design descriptions, including requirements and restrictions (e.g., interface requirements and site design parameters), set forth in Tier 1 and Tier 2 (FSAR) of the DC application, meet the acceptance criteria. The primary reviewer will coordinate this review with the other technical branch areas of review as stated in Section I to address review interfaces. The primary reviewer obtains and uses such input as necessary to ensure that this review procedure is complete.

For the review of a COL or OL application, the scope of the review is dependent on whether the applicant references a certified design or other NRC approvals (e.g., manufacturing license, site suitability report, ESP, or topical report). The design descriptions of physical security systems not addressed by a referenced DC are addressed in the COL and reviewed for how the applicant plans to meet the requirements of 10 CFR Part 73 for physical protection.

On the basis that the regulatory requirements of 10 CFR Part 73 apply to physical security for a nuclear power reactor under either of the licensing processes of 10 CFR Part 50 or 10 CFR Part 52, the procedures and guidance in this SRP section apply to staff review of the design pf physical security systems in the determination on whether to issue an operating license pursuant to 10 CFR Part 50 or a COL pursuant to 10 CFR Part 52. Likewise, the procedures and guidance in this SRP section also are applied in the staff review of changes or

revisions to the design of physical security systems provided to meet performance and prescriptive regulatory requirements.

IV. EVALUATION FINDINGS

For DC application reviews, the findings will summarize the staff's evaluation of requirements and restrictions (e.g., interface requirements and site parameters) and COL action items relevant to this SRP section. The evaluation findings at the DC stage should be substantially equivalent to the following statement:

> For the reasons set forth above, the staff concludes that the applicant has considered and provided physical protection systems or features in the standard **[insert name]** design, within the scope of the standard plant design, to facilitate the implementation of a physical protection program to protect against potential acts of radiological sabotage. As further set forth above, the **[insert applicant]** proposed **[insert name]** standard design has adequately described the plant layout for physical protection and identified vital equipment and areas for meeting, in part, specified requirements of 10 CFR 73.55. As set forth above, the technical bases, including assumptions, are adequately described and provide support of ITAAC for physical protection systems and hardware.
>
> As explained above, the applicant's proposed design of physical protection systems, including system location and configuration, is adequate with respect to the nuclear island and structures (and additional specified plant areas) within the scope of the standard plant design. As also explained above, the application includes technical detail, including design basis information, adequate to allow for completion of the detailed design and verification of the adequacy of construction and installation (ITAAC verification) in accordance with the requirements of 10 CFR Part 52. This conclusion is limited to the adequacy of applicant description of the design bases of the physical protection systems and features within the scope of the standard design that are relied on to implement security response functions (i.e., detection, assessment, communications, security response—delays, interdictions, and neutralization). The demonstration of high assurance of adequate protection against the DBT required by NRC regulations and compliance with the programmatic requirements (including administrative controls such as people and procedures) of NRC regulations for physical protection are to be addressed by a COL applicant that is seeking a COL to construct and operate a nuclear power plant.

The above findings should be modified, as appropriate, to apply to a review of an OL or COL application.

V. IMPLEMENTATION

The staff will use this SRP section in performing safety evaluations of DC applications submitted by applicants under 10 CFR Part 52. In addition, the staff will also use the guidance and procedures described in this SRP in review confirming design of physical security systems meeting the applicable regulatory requirements of 10 CFR Part 73 in security plans and changes to security plans. 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 herein to evaluate conformance with Commission regulations.

This SRP section also applies to the review of design of physical security systems (i.e., engineered controls) within licensing bases established for meeting regulatory requirements applicable to licenses issued or application for license pursuant to 10 CFR Part 50.

VI. REFERENCES

1. National Institute of Justice, "Ballistic Resistant Protective Materials," NIJ Standard 0108.01, Washington, DC.

2. Sandia National Laboratory, "Entry/Exit Control Components for Physical Protection System," NUREG/CR-5899 (SAND 92-1339). Albuquerque, NM.

3. U.S. Department of Defense, "Structures to Resist the Effects of Accidental Explosion," TN 5-1300, (Also designated as Air Force ARF 08-22 and Navy NAVFAC P-2897), Washington, DC.

4. U.S. Department of Energy, Sandia National Laboratories, "Technology Transfer Manuals": SAND2001-2168, "Access Delay Technology, Volume 1," SAND2000 2142, "Entry Control and Contraband Detection Systems," SAND99-2388, "Interior Intrusion Detection," SAND99-2389, "Video Assessment," SAND99-2390, "Alarm Communication," SAND99-2391, "Exterior Intrusion Detection," SAND99-2392, "Protecting Secure Communications," and SAND99-2486, "Explosives Protection," Albuquerque, NM.

5. U.S. Nuclear Regulatory Commission "Combined License Application for Nuclear Power Plants (LWR) Edition," Regulatory Guide 1.206, Agencywide Documents Access and Management System (ADAMS) Accession No ML070720184.

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

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 a Vehicle 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 Meets10 CFR 73.55 Requirements," as it relates to the design of physical security systems, Regulatory Guide 5.69, ADAMS Accession No. ML13151A355.

10. 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.

11. U.S. Nuclear Regulatory Commission, "Physical Protection Programs at Nuclear Power Reactors," Regulatory Guide 5.76, ADAMS Accession No. ML13151A355.

12. U.S. Nuclear Regulatory Commission, “Insider Mitigation Program,” Regulatory Guide 5.77, ADAMS Accession No. ML13151A355.

13. 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.

14. U.S. Nuclear Regulatory Commission, “High Security Protected and Vital Area Barrier/Equipment Penetration Manual,” Regulatory Information Summary 2003-06.

15. U.S. Nuclear Regulatory Commission, “Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants,” Federal Register, Vol. 50, p. 32138, August 8, 1985.

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

17. U.S. Nuclear Regulatory Commission, “Intrusion Detection Systems and Subsystems,” NUREG-1959, November 2010, ADAMS Accession No. ML11112A009.

18. U.S. Nuclear Regulatory Commission, “Protection against Malevolent Use of Vehicles at Nuclear Power Plants,” NUREG/CR-6190, April 2013. ADAMS Accession No. ML13122A181.

19. U.S. Nuclear Regulatory Commission, “Vehicle Barriers: Emphasis on Natural Features,” NUREG/CR-4250.

20. U.S. Nuclear Regulatory Commission, “Nuclear Power Plant Security Assessment Format and Content Guide,” NUREG/CR-7145. ADAMS Accession No. ML13122A181.

21. Underwriters Laboratories, Inc., “Standard for Bullet-Resisting Equipment,” UL 752.

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 number 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.

SRP Section 13.6.2
Description of Changes

Section 13.6.2 "Physical Security - Review Of Physical Security System Designs - Standard Design Certification and Operating Reactor Licensing Applications"

This Revision 2 to the Standard Review Plan, Section 13.6.2 updates Revision 1 of this section, dated October 2010, to incorporate changes in Sections I, II, III, IV, and VI related to the following:

1. Establish the regulatory basis for physical security review for a DC application pursuant to Subpart B of 10 CFR Part 52 and regulatory basis for licensing reviews to confirm applicable requirements of 10 CFR Part 73 are met under either of the licensing processes of 10 CFR Part 50 or 10 CFR Part 52 for a nuclear power reactor.

2. Clarify the scope for a DC review and level of details for designs of physical security systems. Remove discussions in current guidance addressing administrative controls, programs, and management systems, which are addressed in the review of a COL. Remove the term "voluntary," the discussion on target sets, and other regulatory requirements that do not apply to the design of physical security systems, to clarify the scope of a DC review and identify those regulatory requirements applicable in such a review.

3. Enhance staff guidance regarding the scope of review for a DC application (i.e., standard design scope and design details based on RG 1.206 and the FSAR level of detail required for Commission findings). Revise tables to indicate design description and requirements applicable for the designs of physical security systems within and outside of the nuclear island and structures.

4. Identify review interfaces based on topical and subject areas addressed in other NUREG-0800 SRP sections for engineered systems that are relied on to perform physical security functions or support functions for physical security systems. Update guidance on review interfaces with SRP 13.6.1, SRP 13.6.3, and SRP 14.3.12, as they relate to physical security systems, and address other sections of NUREG-0800. Clarify the review interfaces between these SRP sections and SRP Section 14.3.12, which addresses PS-ITAAC, and update guidance regarding COL information items.

5. Update and establish acceptance criteria based on all performance-based and prescriptive regulatory requirements in 10 CFR 73.55 that are applicable to the design of physical security systems, including the regulatory basis for DC based on 10 CFR Part 52.

6. Update technical rationale based on applying acceptance criteria for areas of review that are rooted in the regulations for licensing, specific requirements for DC, and security requirements applicable to nuclear power reactors. Establish a technical rationale for acceptable level of detail for design descriptions for a DC application and conformance with RG 1.206.

7. Update guidance in review procedures for DC and establish specific standards for physical security reviews of descriptions of the detail of designs and design bases for meeting the performance and prescriptive regulatory requirements of 10 CFR 73.55.

8. Revise evaluation findings to reflect the limitations of the approvals available in connection with DC to address only design descriptions of physical security systems within the scope of the DC application.

9. Revise listing of references to guidance that are related to the design of physical security systems and list in a hierarchy of NRC (RG, generic communications, policy statements, NUREGs) and external guidance.

The revision considered the licensing experience from physical security reviews of DC applications for new large light-water reactor (LWR) designs (e.g., the U.S. Evolutionary Pressurized Reactor (U.S. EPR), U.S. Advanced Pressurize Water Reactor (U.S. APWR), the NRC security regulatory framework applicable to the licensing of nuclear power reactors, including small modular reactors (integrated pressurized water reactors and advanced reactors), as discussed in SECY-11-0184, “Security Regulatory Framework for Certifying, Approving, and Licensing Small Modular Nuclear Reactors (M110329)” (Agencywide Documents Access and Management System (ADAMS) Accession No. ML112991113), and the Reactor Security Licensing Branch Working Group assessment results and recommendations on physical security licensing reviews for issuing power reactor licenses (ADAMS Accession No. ML12221A093).

APPENDIX A

Table 13.6.2.2: Designs of Physical Protection Systems for Plant Areas Beyond the Nuclear Island and Structures

Design ID.	Descriptions of Designs	Requirement
2.1	Physical security systems designed to provide or facilitate the capabilities to detect, assess, interdict, and neutralize; design for defense-in-depth of through the integration of systems, technologies, and equipment – as it relates to the design of physical security systems for interior detection, assessment, access control, and security response.	10 CFR 73.55(b)(3)(i) 10 CFR 73.55(b)(3)(ii)
2.2	Specific use, type, function, and placement of physical barriers needed to satisfy the physical protection program design requirement of 10 CFR 73.55(b) and satisfy definition of 10 CFR 73.2, “Definitions.”	10 CFR 73.55(e) 10 CFR 73.2
2.3	Physical barriers necessary to control (or deny) access into plant areas to satisfy the physical protection program design requirements of 10 CFR 73.55(b).	10 CFR 73.55(e)(1)(i)
2.4	Physical barriers provided to protect against the DBT and specific design functions.	10 CFR 73.55(e)(3)(i)(A)
2.5	Physical barriers providing deterrence, delays, and support of access controls.	10 CFR 73.55(e)(3)(ii)
2.6	Physical security systems for securing and monitoring of openings in any barrier system to prevent exploitation of the opening.	10 CFR 73.55(e)(4)
2.7	Bullet-resisting barriers for locations within last access control function for access to the protected area.	10 CFR 73.55(e)(5)
2.8	Physical barriers in the owner control area needed to satisfy the physical protection program design requirements of 10 CFR 73.55(b).	10 CFR 73.55(e)(6)
2.9	Isolation zone configurations and dimensions to permit observation and assessment of activities on either side of the protected area.	10 CFR 73.55(e)(7)(i)(A)
2.10	Intrusion detection systems and equipment to satisfy requirements of 10 CFR 73.55(i) and design for capabilities to detect both attempted and actual penetration of the protected area perimeter barriers, before completed penetration.	10 CFR 73.55(e)(7)(i)(B)
2.11	Assessment equipment to satisfy the requirements of 10 CFR 73.55(i) and provide real-time and play-back/recorded video images of detected activities before and after each annunciation.	10 CFR 73.55(e)(7)(i)(C)
2.12	Design to address obstructions that could prevent the capabilities for observation and assessment located outside the isolation zone.	10 CFR 73.55(e)(7)(ii)

2.13	Physical barriers for the protected area perimeter to limit access into the protected area, channeling personnel, vehicle, and material to designated access control portals, and separation of protected area barriers from designated vital area physical barriers.	10 CFR 73.55(e)(8) 10 CFR 73.55(e)(8)(i)(A) through 73.55(e) (8)(i)(C)
2.14	Securing and monitoring protected area barriers that delay and prevent exploitation of penetrations.	10 CFR 73.55(e)(8)(ii)
2.15	Alarm and secure by locking device that allows prompt egress of all emergency exits on the protected area barrier systems.	10 CFR 73.55(e)(8)(iii)
2.16	Physical barrier, detection, and assessment systems where building walls or roof comprise a portion of the protected area perimeter barrier and an isolation zone is not provided.	10 CFR 73.55(e)(8)(iv)
2.17	Identify list of vital equipment and designated vital area barriers located outside of the nuclear island and structures.	10 CFR 73.55(e)(9)(i)
2.18	Intrusion detection equipment and locking devices for rapid egress during emergency and satisfy the vital areas entry controls.	10 CFR 73.55(e)(9)(ii)
2.19	Unoccupied vital areas are locked and alarmed.	10 CFR 73.55(e)(9)(iii)
2.20	Identify locations of the central alarm station (CAS), secondary alarm station (SAS), secondary power supply systems for alarm annunciation equipment, secondary power supply system for nonportable communications equipment and designated vital area barriers, if located outside the nuclear island and structures.	10 CFR 73.55(e)(9)(v) 10 CFR 73.55(e)(9)(vi)
2.21	Vehicle control measures to protect against the DBT vehicle bomb assault, vehicle barrier systems (including passive and active barriers) at adequate standoff distance, secondary power source, or a means of mechanical or manual operations of active barrier systems, and surveillance and observation of vehicle barriers.	10 CFR 73.55(e)(10) 10 CFR 73.55 (e)(10)(i)(A) and (e)(10)(i)(B)
2.22	Installation of train derailer, remove track, or restrict access to railroad sidings, where applicable	10 CFR 73.55(e)(1)(i)(D)
2.23	Restriction of waterborne vehicles.	10 CFR 73.55(e)(10)(ii)(A)
2.24	Location of access portal outside of, or concurrent with, the physical barrier systems.	10 CFR 73.55(g)(1) (i)(A)
2.25	Access control portals with locking devices, intrusion detection, and surveillance equipment; and physical security systems for supervision and controls to prevent unauthorized bypass of access control equipment located at or outside of the PA. Also design the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions.	10 CFR 73.55(g)(1)(i)(B) 10 CFR 73.55(g)(1)(i)(C) 10 CFR 73.55(g)(5)(i)
2.26	Bullet-resisting structure for the last access control	10 CFR 73.55(g) (1)(i)(E)

	functions (e.g., controlling admission to the protected area).	
2.27	Physical security systems for conducting searches for control areas and physical protection program to detect, deter, and prevent introduction of fire arms, explosives, incendiary devices, or other items that could be used to commit radiological sabotage at each access control point of portal.	10 CFR 73.55(h)(3)
2.28	Video surveillance systems and capabilities monitored by an individual capable of initiating a response at vehicle access control points.	10 CFR 73.55(h)(2)(v)
2.29	Detection and assessment systems that satisfy the design requirement of 10 CFR 73.55(b), outside of the nuclear island and structures.	10 CFR 73.55(i)
2.30	Intrusion detection equipment annunciations and video assessment displays, in at least two onsite alarm stations. Design of systems for visual and audible annunciation of alarm, visual display for assessment, annunciation of alarm types and locations, tamper indications and self-checking of transmission lines, automatic indication of system or a component of alarm system failure and operating on backup power supply, and support initiation of security response.	10 CFR 73.55(i)(2) 10 CFR 73.55(i)(3)(i) 10 CFR 73.55(i)(3)(ii) 10 CFR 73.55(i)(3)(iii) 10 CFR 73.55(i)(3)(iv) 10 CFR 73.55(i)(3)(v) 10 CFR 73.55(i)(3)(vii)
2.31	Protection of at least one alarm station against a single act in accordance with the DBT to ensure survivability of at least one alarm station.	10 CFR 73.55(i)(4) (i)
2.32	Locate the CAS inside the protected area and the interior of the CAS must not be visible from the perimeter of the protected area, if the CAS is located outside the nuclear island and structures.	10 CFR 73.55(i)(4)(ii)(A)
2.33	Controls for status of detection points or deactivated locking or access control devices at protected or vital area portal cannot be changed without the knowledge concurrences, and indications of all alarms' final disposition.	10 CFR 73.55(i)(4)(ii)(F)
2.34	Equal and redundant CAS and SAS, such that all functions needed can be performed in both alarm stations.	10 CFR 73.55(i)(4)(iii)
2.35	Systems providing capabilities for surveillance, observations, and monitoring to satisfy the design requirements of 10 CFR 75.55(b), outside of the nuclear island and structures.	10 CFR 73.55(i)(5)(i)
2.36	Continuous surveillance, observations, and monitoring of the owner controlled areas, if video technology is applied.	10 CFR 73.55(i)(5)(ii)
2.37	Physical barriers and intrusion detection monitoring of unattended openings that intersect a security boundary, outside of the nuclear island and structures.	10 CFR 73.55(i)(5)(iii)

2.38	Specification for illumination necessary to satisfy the design requirement of 10 CFR 73.55(b), minimum illumination level of a 0.2-foot candle, and design basis for how lighting requirements are met. Where applicable, the type(s) and application of low-light technologies for all areas outside of the nuclear island and structures.	10 CFR 73.55(i)(6)(i) 10 CFR 73.55(i)(6)(iii)
2.39	Systems for continuous communications with onsite and offsite resources; communications capabilities terminate in both alarm stations; radio or microwave transmitted two-way voice communication, conventional telephone; communication with reactor control room; and independent power source for non-portable communication equipment, outside of the nuclear island and structures.	10 CFR 73.55(j)(1) 10 CFR 73.55(j)(4) 10 CRR 73.55(j)(4)(i) 10 CFR 73.55(j)(4)(ii) 10 CFR 73.55(j)(5) 10 CFR 73.55(j)(6)