U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-5076

Proposed new Regulatory Guide 5.97

Issue Date: XXXXX XXXX
Technical Lead: Stacy Prasad

The U.S. Nuclear Regulatory Commission (NRC) is making this document publicly available for information only concurrent with the Commission's review of SECY-23-0021, "Proposed Rule: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors" (ADAMS Accession No. ML21162A095). The contents of this document are subject to change and should not be interpreted as official agency positions.

The NRC is not seeking public comment on this document.

If the Commission approves the publication of the proposed rule, then the *Federal Register* notice of proposed rulemaking will provide an opportunity for the public to submit formal comments on the proposed rule and draft guidance. Please note that any Commission approval for the publication of the proposed rule may result in changes to this document.

GUIDANCE FOR TECHNOLOGY-INCLUSIVE REQUIREMENTS FOR PHYSICAL PROTECTION OF LICENSED ACTIVITIES AT COMMERCIAL NUCLEAR PLANTS

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes methods and approaches that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for meeting the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 53, "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants" (Ref. 1). It provides guidance for meeting the requirements for physical protection of licensed activities at commercial nuclear plants against radiological sabotage.

Applicability

This RG applies to applicants and holders of a license under the provisions of 10 CFR Part 53 and applicable provisions of 10 CFR Part 73, "Physical Protection of Plants and Materials" (Ref. 2).

This RG is being issued in draft form to involve the public in the development of regulatory guidance in this area. It has not received final staff review or approval and does not represent an NRC final staff position. Public comments are being solicited on this RG and its associated regulatory analysis. Comments should be accompanied by appropriate supporting data. Comments may be submitted through the Federal rulemaking website, http://www.regulations.gov, by searching for draft regulatory guide DG-5076. Alternatively, comments may be submitted to Office of the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Rulemakings and Adjudications Staff. Comments must be submitted by the date indicated in the *Federal Register* notice.

Electronic copies of this RG, previous versions of RGs, and other recently issued guides are available through the NRC's public website under the Regulatory Guides document collection of the NRC Library at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html. The RG is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML22203A131. The regulatory analysis is associated with a rulemaking and may be found in ML21165A112.

Applicable Regulations

- 10 CFR Part 53 provides an alternative risk-informed and technology-inclusive regulatory framework for the licensing, construction, operation, and decommissioning of commercial nuclear plants.

    - 10 CFR 53.860, "Security programs," requires that each nuclear power reactor licensee or applicant under 10 CFR Part 53, Framework A, establish, maintain, and implement a physical protection program.

    - 10 CFR 53.4330, "Security programs," requires that each nuclear power reactor licensee or applicant under 10 CFR Part 53, Framework B, establish, maintain, and implement a physical protection program.

- 10 CFR Part 73 prescribes requirements for the establishment and maintenance of a physical protection system for the protection of special nuclear material (SNM) at fixed sites and in transit.
    - 10 CFR 73.1, "Purpose and scope," requires that licensees establish and maintain a physical protection system that will have capabilities for the protection of SNM at fixed sites and in transit and of plants in which SNM is used.

    - 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," contains requirements for certain power reactor licensees for establishing and maintaining a physical protection program that provides high assurance that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety.

    - 10 CFR 73.56, "Personnel access authorization requirements for nuclear power plants," requires certain power reactor licensees to establish, implement, and maintain an access authorization program and implement the requirements of this section through its Commission-approved physical security plan.

    - 10 CFR 73.58, "Safety/security interface requirements for nuclear power reactors," requires the licensee to assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security.

    - 10 CFR 73.100, "Technology-inclusive requirements for physical protection of licensed activities at commercial nuclear plants against radiological sabotage," affords certain commercial nuclear plant licensees flexibility in designing and implementing a physical protection program to protect the security of the plant and nuclear materials.

    - 10 CFR Part 73, Appendix B, "General Criteria for Security Personnel," Section VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," describes minimum training and qualification requirements that must be implemented through a Commission-approved training and qualification plan.

    - 10 CFR Part 73, Appendix C, "Licensee Safeguards Contingency Plans," describes requirements for a documented plan to give guidance to licensee personnel to accomplish

specific defined objectives in the event of threats, thefts, or radiological sabotage relating to nuclear power reactors.

Related Guidance[1]

- RG 5.12, "General Use of Locks in the Protection and Control of: Facilities, Radioactive Materials, Classified Information, Classified Matter, and Safeguards Information and Special Nuclear Materials" (Ref. 3), provides criteria that the NRC staff considers acceptable for the selection and use of commercially available locks in the protection of facilities and SNM.

- RG 5.44, "Perimeter Intrusion Alarm Systems" (Ref. 4), describes the functions of perimeter intrusion detection sensors and detection methods and systems testing that the NRC staff considers acceptable for meeting provisions contained in the requirements of 10 CFR 73.55(i), 10 CFR 73.55(n), 10 CFR 73.100(b)(3)(i), and 10 CFR 73.100(b)(3)(ii).

- RG 5.54, "Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants (SGI)" (Ref. 5). Note that RG 5.54 contains safeguards information (SGI) and is, therefore, not publicly available.

- RG 5.66, "Access Authorization Program for Nuclear Power Plants" (Ref. 6), describes methods and processes that the NRC staff considers acceptable for meeting the requirements of 10 CFR 73.56 and 10 CFR 73.57, "Requirements for criminal history background checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to Safeguards Information."

- RG 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements (SGI)" (Ref. 7), describes methods the NRC staff considers acceptable for satisfying the general performance objectives and requirements in 10 CFR 73.55. Note that RG 5.69 contains SGI and is, therefore, not publicly available.

- RG 5.71, "Cyber Security Programs for Nuclear Facilities" (Ref. 8), provides an approach that the NRC staff considers acceptable for complying with the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks," with regard to a cyberattack, including that associated with the design-basis threat (DBT) of radiological sabotage.

- RG 5.74, "Managing the Safety/Security Interface" (Ref. 9), provides methods and processes that the NRC staff considers acceptable for managing the interface between plant operational functions and security functions and meeting the requirements of 10 CFR 73.58.

- RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities" (Ref. 10), provides an approach that the NRC staff considers acceptable for complying with the requirements of 10 CFR Part 73, Appendix B, for training, equipping, testing, qualifying, and requalifying armed and unarmed security personnel, watchpersons, and other members of the

1 Applicants, licensees, and combined license (COL) holders should consider the following related guidance when using this RG to assist in the development and preparation of applications. Although some guidance documents are written mainly for light-water nuclear power reactors and are based on the criteria of risk for core damage, the designers and applicants may find the approaches described therein as useful in developing accident consequence assessments and characterizing the source terms for a given design and application. The staff may use the guidance as applicable in the review of the applicants' approaches for the given subject areas.

licensee's security organization to ensure that these individuals possess and maintain the knowledge, skills, and abilities required to carry out their assigned duties and responsibilities effectively.

- RG 5.76, "Physical Protection Programs at Nuclear Power Reactors (SGI)" (Ref. 11), describes methods and processes that the NRC staff considers acceptable for generally meeting the requirements of 10 CFR 73.55. Note that RG 5.76 contains SGI and is, therefore, not publicly available.

- RG 5.77, "Insider Mitigation Program" (Ref. 12), describes methods and processes that the NRC staff considers acceptable for implementing an effective insider mitigation program required in 10 CFR 73.55(b)(9) and 10 CFR 73.100(b)(9).

- DG-5071 (revised RG 5.81), "Target Set Identification and Development for Nuclear Power Reactors," issued December 2019 (Ref. 13), describes methods that the NRC staff considers acceptable for meeting the requirements of 10 CFR 73.55(f) for applicant or licensee analysis, development documentation, and reevaluation of target set elements and target sets, including preventive operator actions that may be credited to prevent core damage (e.g., nonlocalized fuel melting, core destruction) or spent fuel coolant and exposure of spent fuel. Note that RG 5.81 is designated as Official Use Only—Security-Related Information and is, therefore, not publicly available.

- DG-5072 (proposed new RG 5.90), "Guidance for Alternative Physical Security Requirements for Modular Reactors and Non-Light-Water Reactors" (Ref. 14), provides an acceptable method that applicants and licensees may use in determining if they are eligible to use one or more of the preliminary, proposed alternative physical security requirements described in SECY-22-0072 (ADAMS Accession No. ML21334A003) and guidance for implementing those requirements.

- NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (Ref. 15), provides guidance to NRC staff in performing safety reviews of construction permit or operating license applications under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 16), and early site permit, design certification, COL, standard design approval, or manufacturing license applications under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 17).

    - Section 13.6.1, "Physical Security—Combined License and Operating Reactors," provides the staff guidance for the review of engineered physical security systems, hardware, and features; administrative controls; and management systems for operations and organization.

    - Section 13.6.2, "Physical Security—Design Certification," provides guidance for the physical security review of designs of physical security systems.

    - Sections 13.6.1 and 13.6.2 describe a comprehensive physical security program for COL applicants and operating reactor licensees.

- NUREG/CR-7145, "Nuclear Power Plant Security Assessment Guide," issued April 2013 (Ref. 18), describes an acceptable approach for performing security assessments to demonstrate that the physical protection system design of a new reactor facility provides assurance of protection against the DBT of radiological sabotage.

- NUREG-1964, "Access Control Systems: Technical Information," issued April 2011 (Ref. 19), provides technical details applicable to the application, use, function, installation, maintenance, and testing parameters for access control and search equipment and the implementation of protective measures that support access control.

- NUREG/CR-7201, "Characterizing Explosive Effects on Underground Structure," issued September 2015 (Ref. 20), provides technical guidance on characterizing the effects that explosions close to the ground surface or in contact with the ground surface have on underground structures for designs to protect against the explosives.

- NUREG/CR-6190, Revision 1, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants," Volume 1, "Vehicle Barrier System Siting Guidance for Blast Protection," and Volume 2, "Vehicle Barrier System Selection Guidance," both issued December 1994 (Ref. 21), provide a simplified procedure for selecting land vehicle barriers that will stop the design-basis vehicle threat.

- U.S. Department of Energy (DOE), Sandia National Laboratories, SAND2001-2168, "Technology Transfer Manual—Access Delay Technology, Volume 1," issued 2001 (Ref. 22), provides technical guidance on access delay systems to impede a group of well-equipped and dedicated adversaries for a length of time to enable the response force opportunities to interdict and neutralize.

- DOE, SAND2008-5644, "Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants," issued 2008 (Ref. 23), describes a systematic process involving logic models to identify the minimum set of areas that must be designated as vital areas to ensure that all radiological sabotage scenarios are prevented.

- DOE, SAND2007-5591, "Security Assessment Technical Manual," issued September 2007 (Ref. 24), provides conceptual and specific technical guidance for the development of the layout of a facility to enhance protection against sabotage and facilitate the use of physical security features, design the physical protection system to be used at the facility, and analyze the effectiveness of the physical protection system against the DBT.

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses. Regulatory guides are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs are acceptable if supported by a basis for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides voluntary guidance for implementing the mandatory information collections in 10 CFR Part 53 and 10 CFR Part 73 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget (OMB), under control number 3150-XXXX and 3150-0002, respectively. Send comments regarding this information collection to the FOIA, Library, and Information Collections Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to

Infocollects.Resource@nrc.gov, and to the OMB Office of Information and Regulatory Affairs, Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

TABLE OF CONTENTS

B. DISCUSSION

Reason for Issuance

The current application and licensing requirements, developed for large light-water reactors (LWRs) as outlined in 10 CFR Part 50 and 10 CFR Part 52, do not fully consider the variety of designs for nuclear reactors and may require extensive use of the exemption process for regulations that include prescriptive requirements specific to LWRs. Therefore, the NRC has created an alternative regulatory framework in 10 CFR Part 53 for licensing nuclear reactors and a corresponding regulation for implementing performance-based security requirements in 10 CFR 73.100. The requirements found in 10 CFR 73.100 are less prescriptive and less restrictive on the licensee in its design of the physical protection systems and provide flexibility to allow for methods other than those prescribed in 10 CFR 73.55.

Background

This RG is for applicants and licensees that are licensed under the provisions of 10 CFR Part 53, to use as guidance for the following:

- complying with 10 CFR 53.440(f) safety and security design process considerations
- determining eligibility for meeting the performance criterion in 10 CFR 53.860 or 10 CFR 53.4330 to relieve the applicant from the applicable requirements to defend against radiological sabotage outlined in 10 CFR 73.55 or 10 CFR 73.100
- applying the physical security requirements of 10 CFR 73.100, as an alternative to 10 CFR 73.55 for protection against radiological sabotage

This guidance provides acceptable methods for applying security measures in the design of a physical protection program. Each licensee should account for and determine whether additional measure(s) are needed for compliance with the applicable requirements in 10 CFR Part 53 and 10 CFR Part 73. The licensee is ultimately responsible for ensuring that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety.

The licensee should ensure that information submitted to the NRC describes the physical protection program completely and accurately and is documented in the physical security plan. The security plan establishes engineered systems, administrative controls, management systems, and an organization for a physical protection program that provides the necessary protection against malevolent acts and DBT acts of radiological sabotage and indicates how the licensee complies with regulatory requirements. The security plan provides the licensing basis for the Commission's determination that the issuance of the license will not be inimical to the common defense and security or to public health and safety. The physical security program provides reasonable assurance that the plant and activities involving SNM and operations are as analyzed and within the safety envelope described in the final safety analysis report and do not constitute an unreasonable risk to public health and safety.

The applicant's or licensee's physical security plan contains information that is part of the licensing basis required by 10 CFR Part 53. The security plan provides written commitments for ensuring compliance with applicable NRC requirements in the conduct of nuclear operations. The physical security plan and supporting documents (such as security assessments and blast analysis) are required to be

maintained in effect for the life of the operating license or COL. The general performance requirements of 10 CFR 73.55(b) or 73.100(b) and the prescriptive requirements applicable to a commercial nuclear plant in 10 CFR Part 73 require licensees and applicants to establish and maintain a physical protection program that includes a security organization. The descriptions of the design of a physical protection program, including the specific proposed design of engineered and administrative controls, management systems, and the security organization are required to meet the performance and prescriptive requirements in 10 CFR 73.55 or 73.100.

Applicants requesting a license under 10 CFR Part 53 are required to meet the provisions set forth in either 10 CFR 73.55 or 10 CFR 73.100 for protection against the DBT of radiological sabotage, unless the licensee meets the criterion in 10 CFR 53.860(a)(2)(i) or 10 CFR 53.4330(a)(2)(i):

> (i) The radiological consequences from a design-basis-threat initiated event involving the loss of engineered systems for decay heat removal and possible breaches in physical structures surrounding the reactor, spent fuel, and other inventories of radioactive materials result in offsite doses below the values in § 53.210 [or 53.4730(a)(1)(vi)] of this chapter.

This guidance document includes methods the NRC staff deems acceptable for satisfying the criterion in 10 CFR 53.860(a)(2)(i) and (a)(2)(ii) or 10 CFR 53.4330(a)(2)(i) and (a)(2)(ii) for the site-specific analysis, as follows:

> (ii) The applicant must perform a site-specific analysis, including identification of target sets, to demonstrate that the criterion in § 53.860(a)(2)(i) [or 53.4330(a)(2)(i)] is satisfied. The analysis must assume that licensee mitigation and recovery actions, including any operator action, are unavailable or ineffective. The licensee must maintain the analysis until the permanent cessation of operations and permanent removal of fuel from the reactor vessel as described under § 53.1070 [or 53.4670].

This guidance also describes methods the NRC staff deems acceptable to demonstrate compliance with 10 CFR 53.860(a)(1) or 10 CFR 53.4330(a)(1), as follows:

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

Should the applicant, licensee, or COL holder be unable to demonstrate its ability to satisfy 10 CFR 53.860(a)(2)(i) or 10 CFR 53.4330(a)(2)(i), this guidance includes methods the NRC staff deems acceptable to demonstrate compliance with the performance-based, technology-neutral physical security requirements in 10 CFR 73.100 for commercial nuclear plants. This document does not provide guidance to implement 10 CFR 73.55, however, because other guidance documents are available, such as RG 5.76 and RG 5.69.

If used by the applicant, licensee, or COL holder, the methods and approaches described in this guidance document would provide assurance that the required security licensing basis complies with the regulatory requirements that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety.

Consideration of International Standards

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA has established a series of security guides to address nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities. IAEA security guides present international good practices and increasingly reflect best practices to help users striving to achieve high levels of security. To inform its development of this RG, the NRC considered IAEA Safety Requirements and Safety Guides pursuant to the Commission's International Policy Statement (Ref. 25) and Management Directive and Handbook 6.6, "Regulatory Guides" (Ref. 26).

The following IAEA Nuclear Security Series documents were considered in the development of this RG. These documents largely recommend a risk-informed approach appropriate for the new regulatory framework:

- IAEA Nuclear Security Series No. 27-G, "Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)," Implementing Guide, issued 2018 (Ref. 27)

- IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," Recommendations, issued 2011 (Ref. 28)

- IAEA Nuclear Security Series No. 40-T, "Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities," Technical Guidance, issued 2021 (Ref. 29)

C. STAFF REGULATORY GUIDANCE

This section provides the methods that the staff considers acceptable for meeting the requirements of the regulations cited in the Introduction.

1. Security by Design (10 CFR 53.440(f))

1.1 In accordance with 10 CFR 53.440(f), safety and security are required to be considered together in the design process such that, where possible, security issues are effectively resolved through design and engineered security features. In accordance with 10 CFR 53.1239(a)(14), an applicant is required to submit "confirmation that safety and security were considered together in the design process, as required by 10 CFR 53.440(f)."

1.2 The design of reactor plant structures, systems, and components (SSCs) and site layout should include, to the extent practical, interfaces with designs of physical security systems meeting 10 CFR Part 73, to more efficiently enable engineered and administrative security functions to meet requirements. The consideration of safety and security in the facility design phase should result in security features—including coordination with safety operations—to enhance the efficiency and effectiveness of reactor and facility security performance. Such a design should include, to the extent practical, the following:

- locating reactor and critical safety and supporting SSCs below ground to facilitate protection against vehicle-borne explosive threats and external ground assaults, and to minimize points to access vital equipment and operations areas;
- incorporating physical security features that improve the ability to observe, assess, and monitor plant areas, such as locking devices and intrusion detection devices;
- configuring site layout and facility structures to maximize defensive fighting positions by overlapping fields of fire and minimizing obstructions for lines of sight for neutralization functions;
- hardening and configuring interior and exterior walls and openings (e.g., doors; windows; heating, ventilation, and air conditioning (HVAC); utility penetrations; pipes) to protect against breaching;
- implementing a reliable and available backup power supply for continuity of physical security functions;
- implementing reliable and available normal and emergency lighting for performing security assessment, interdiction, and neutralization functions;
- using human factors to increase attentiveness and effectiveness of security responders;
- configuring engineering and administrative features to enhance insider threat mitigation approaches, such as tamper indicating systems;
- designing for personnel protection or survivability against hazards such as radiological, chemical, and fire hazards by including, for example, high efficiency particulate air filtration, recirculation and fresh air supply, fire-rating, bullet-resistant materials, differential pressures, and HVAC isolation dampers;

- implementing security features that address vulnerabilities of emergency egress routes; and

- configuring site layout and buildings to protect against blast effects, including overpressure impacting structural integrity, from DBT adversary land and waterborne vehicle explosive threats.

Additional guidance in this subject area appears in documents such as the following:

- RG 5.74

- U.S. Army Corps of Engineers (USACE) Protective Design Center Technical Report PDC-TR-06-09, "Vehicle Access Control Point Guidance," issued 2008 (Ref. 30)

- SAND2007-5591

- SAND2000-2142, "Technology Transfer Manual—Entry Control and Contraband Detection System," issued 2000 (Ref. 31)

- SAND2021-13779 R, "U.S. Domestic Microreactor Security-by-Design," issued 2021 (Ref. 32)

- SAND2021-13122 R, "U.S. Domestic Pebble Bed Reactor: Security-by-Design," issued 2021 (Ref. 33)

- World Institute for Nuclear Security, Security of Advanced Reactors, Special Report Series, "Secure by Design: Guidance document principles and methods," issued 2020 (Ref. 34)

2. Security Operations Program—10 CFR 53.860 or 10 CFR 53.4330

A commercial nuclear plant licensee under 10 CFR Part 53 that does not meet the criterion in 10 CFR 53.860(a)(2)(i) or 10 CFR 53.4330(a)(2)(i) is required to implement the requirements of 10 CFR 73.55 or 10 CFR 73.100 through its physical security plan, training and qualification plan, safeguards contingency plan, and cybersecurity plan, referred to collectively hereafter as "security plans." The physical security requirements in 10 CFR 73.100 provide a regulatory framework based on performance requirements that minimize or eliminate prescriptive requirements (when compared to 10 CFR 73.55) to permit the applicant or licensee the flexibility to determine how it will design and implement the physical protection necessary to protect against the DBT and ensure security of the plant for activities involving nuclear material. The physical security requirements in 10 CFR 73.55 use a combination of performance criteria (e.g., the physical protection program must ensure that the capabilities to detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage as stated in 10 CFR 73.1, are maintained at all times) and numerous prescriptive requirements developed to achieve the performance objectives. In the performance-based approach to physical security in 10 CFR 73.100, performance criteria and objectives are the primary basis for evaluating the effectiveness of a physical protection program, giving the licensee the flexibility to determine how to meet the established criteria.

2.1 Consequence Analysis for a Design-Basis-Threat-Initiated or Security-Related Event

General Instructions and Assumptions

The license or applicant must perform a site-specific analysis, including identification of target sets, if it intends to demonstrate that it meets the eligibility criterion in 10 CFR 53.860(a)(2)(i) or 10 CFR 53.4330(a)(2)(i). This consequence analysis should calculate the potential radiation doses at the exclusion area boundary (EAB) for any 2-hour period after initiation of the release and at the outer boundary of the low-population zone (LPZ) for the duration of the passage of the plume. These calculated doses are compared to the dose criteria in 10 CFR 53.210 or 10 CFR 53.4730(a)(1)(vi), as applicable.

2.1.1 For this analysis, the licensee or applicant should postulate a bounding event involving the loss of engineered systems for decay heat removal and possible breaches in physical structures surrounding the reactor, spent fuel, and other inventories of radioactive materials. The analysis should describe the initiating security event, any actions taken by the DBT adversary, and the assumptions credited in the analysis. It should provide the calculated source term to include the type and amount of radioactivity potentially released to the environment. The analysis must assume that licensee mitigation and recovery actions (e.g., manual action to trip reactor), including any operator action, are unavailable or ineffective.

2.1.2 The postulated event in the consequence analysis should be based on DBT-initiated or security-related event scenarios for the facility that have the potential to result in a radiological release to the environment.

2.1.3 The analysis should describe any and all scenarios that could result in releases of radionuclides from any source.

2.1.4 A licensee or applicant should use the analysis described in RG 5.81 to identify target sets as a starting point for developing the consequence analysis.

2.1.5 The development of the event scenarios should consider the potential for the adversary to disable any SSCs, barriers, and safety-related equipment required to prevent a radiological release. The analysis should consider both direct and indirect attacks and account for all DBT-related attributes, including available tools, cyber capabilities, insider threats, vehicle bombs, and explosive inventory, as appropriate.

2.1.5.1 The consequence analysis for a direct-attack scenario should do the following:

- Identify the DBT's effect on the physical and chemical characteristics of radiological release (e.g., possible addition of heat formation resulting in atmospheric transfer of radioactive material), as well as release locations.
- Identify radioisotope inventory, release fraction, and respirable fraction.

2.1.5.2 The consequence analysis for the indirect-attack scenarios should do the following:

- Assume the disablement of SSCs and equipment to place radiological material in an unsafe state.
- Assume failure of engineered safety systems to achieve a bounding analysis that considers intentional acts.

- Consider whether pressure, releases, explosions, or other mechanisms could cause a breach of structures indirectly without direct application of the DBT to create a pathway to release.

2.1.6 Licensees or applicants should identify, describe, or refer to the inherent features of the reactor in the licensee's safety evaluation report that would be credited and the mechanisms that would allow the radiological release to be delayed, minimized, or prevented for the DBT-initiated or security-related event scenarios.

2.1.7 For each release scenario for which doses are assessed, the licensee or applicant should develop a quantitative radiological source term by specifying atmospheric release characteristics, such as the time-dependent isotopic release rates to the atmosphere, release durations, release locations, physical or chemical form (including particle size), and plume buoyancy.

2.1.8 The licensee or applicant should describe the physical properties of the source term and released radioactive material (e.g., particle sizes, respirable fractions, heat load) for the specific evaluated DBT-initiated or security-related event scenarios.

2.1.8.1 The analysis should address potential changes to these physical properties from actions that could be taken by the DBT adversary during an attack and discuss how radionuclide transport may or may not be affected.

2.1.8.2 The analysis should address the physical and chemical processes affecting the timing, composition, and magnitude of the release, such as radiative, convective, or conductive cooling; radioactive decay and in-growth corrections; and radionuclide removal or retention processes.

2.1.8.3 The licensee or applicant should demonstrate that radiological sabotage of the source term at the operational location, including anywhere fission-product inventory may exist temporarily outside of the core or core module (e.g., emergency dump tanks, holding tanks, fuel or coolant cleanup systems in molten fuel designs or online continuous fueling systems), would not exceed the dose values. If the radioactive material has more than one operational location, the licensee or applicant should demonstrate that the criterion is satisfied using either the operational location most advantageous to the adversary or every operational location of the material.

2.1.8.4 The consequence analysis should evaluate atmospheric release and direct dose contributors to doses at the EAB and the outer boundary of the LPZ and consider the site characteristics for the specific facility.

- The atmospheric release may be modeled as a neutral density plume that does not undergo chemical or physical transformations after release to the atmosphere, with corrections for radioactive decay and in-growth, wet or dry deposition (or both), and plume rise due to buoyancy or momentum (or both), as appropriate.
- If the chemical or physical form of the atmospheric release requires more complex atmospheric transport modeling due to varying fuel types, materials, and facility design or specifics of the evaluated event scenario, then additional analyses may be needed.

2.1.8.5 The NRC provides further guidance on methods to perform the analysis (e.g., meteorological parameters, atmospheric transport modeling, exposure parameters) in DG-5072 (proposed new RG 5.90).

2.2 Security Requirements if Consequence Criterion Is Met

Consistent with 10 CFR 53.860(a) or 10 CFR 53.4330(a), each applicant that meets the consequence criterion "must implement security requirements for the protection of SNM based on the

type, enrichment, and quantity in accordance with 10 CFR Part 73, as applicable, and implement security requirements for the protection of Category 1 and Category 2 quantities of radioactive material in accordance with 10 CFR Part 37, as applicable."

Additional site-specific security considerations may be warranted based on the category of SNM intended to be used at the facility. These security plans and procedures should be designed to detect, assess, and respond to unauthorized activities. Security plans and procedures should take a defense-in-depth approach and should include controlled access areas (meaning doors to such areas are locked), screening of personnel with unescorted access, lock and key controls, alarms and other devices to detect an unauthorized presence, and rapid-response procedures for first responders (projected to arrive within minutes of alarm). The NRC continues to evaluate and inspect security, material control and accountability, and all other safety- and security-related plans, procedures, and systems to ensure requirements are met.

The physical protection of Category II quantities of SNM is regulated under 10 CFR 73.67, "Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance." However, supplemental physical protection measures may be required for applicants meeting the criterion that are not subject to 10 CFR 73.55 or 10 CFR 73.100 for protection against the DBT of radiological sabotage. The current practice is to conduct case-specific reviews based on the existing regulations and guidance. Possible supplemental security measures may include the following:

- controls over material during use and storage that are not required when the licensee is not subject to the DBT of radiological sabotage,
- consideration of additional controls for material access areas given the potential presence of Category II SNM,
- enhanced background checks,
- enhanced controls for vehicle entry control points,
- enhanced escort requirements,
- random entry searches and enhanced exit searches,
- security patrols,
- enhanced communication and coordination with law enforcement, and
- a security equipment maintenance program.

To ensure a timely and efficient review, applicants should engage with the NRC staff early and often in the licensing process and should provide information about the facility setting, facility processes, types of materials (physical and chemical forms, enrichment, quantity), facility layout, and material flow (transportation, storage, use).

Additionally, applicants satisfying the criterion shall establish, implement, and maintain their access authorization program in accordance with the requirements of 10 CFR 73.120, "Access authorization program for commercial nuclear plants." The NRC provides further guidance in DG-5074, "Access Authorization Program for Commercial Nuclear Plants" (proposed new RG 5.95) (Ref. 35).

3. Security Requirements if Consequence Criterion Cannot Be Met

Consistent with 10 CFR 53.860(a)(2) or 10 CFR 53.4330(a)(2), an applicant that cannot meet the consequence criterion or that chooses not to perform the consequence analysis is required to implement the requirements of 10 CFR 73.55 or 10 CFR 73.100. Section 4 contains further guidance regarding implementation of 10 CFR 73.100. This document does not include relevant guidance for satisfying the requirements of 10 CFR 73.55, as the NRC has issued previous guidance documents the NRC staff finds acceptable for satisfying 10 CFR 73.55, including, but not limited to, RG 5.69 and RG 5.76.

4. 10 CFR 73.100—Performance-Based Framework

Consistent with 10 CFR 53.1369, 10 CFR 53.1413, 10 CFR 53.4969, or 10 CFR 53.5016, each application for an operating license or COL subject to the provisions of 10 CFR 73.100 is required to include a physical security plan, a training and qualification plan, a cybersecurity plan, and a safeguards contingency plan. These four plans combined, referred to collectively hereafter as "security plans," are used to prevent radiological sabotage in accordance with Commission requirements.

In part, 10 CFR 73.100(a) states that each nuclear power reactor licensee shall implement the requirements of 10 CFR 73.100 through its security plans. The security plans are required to identify, describe, and account for site-specific conditions that affect the licensee's capability to satisfy the requirements of 10 CFR 73.100. For example, the licensee is responsible for providing appropriate site-specific details within the plans to adequately describe site-specific conditions and explain how associated regulatory requirements are satisfied by the licensee's physical protection program, including how implementing procedures ensure that required functions are performed effectively. Licensees are responsible for ensuring that the nature of the condition is clearly described, including how the licensee's implementation of the plans would satisfy regulatory requirements.

4.1 General Performance Objective and Requirements

As described in 10 CFR 73.100(b)(1) and (2), the licensee is required to establish, implement, and maintain a physical protection program and a security organization to provide reasonable assurance that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety. To satisfy this general performance objective, the physical protection program is required to protect against the DBT of radiological sabotage as stated in 10 CFR 73.1. Specifically, the licensee is required to ensure that (1) the capabilities to protect against the DBT of radiological sabotage are maintained at all times and (2) defense in depth is provided in achieving performance requirements through the integration of engineered systems, administrative controls, and management measures.

4.1.1 Physical Protection Design Requirements:

The physical protection program is required to achieve and maintain at all times the capabilities for meeting the performance requirements as described in 10 CFR 73.100(b)(3). Physical security SSCs shall be designed to be reliable and available to enable detection, assessment, communication, delay, and neutralization of threats; to protect against internal and external malevolent acts, including the DBT for radiological sabotage; and to protect against the theft or diversion of SNM.

As stated in 10 CFR 73.100(b)(3), the physical protection program must be designed and implemented to achieve and maintain the reliability and availability of SSCs required for meeting the noted performance requirements at all times.

4.1.1.1 Intrusion Detection—10 CFR 73.100(b)(3)(i)

Consistent with 10 CFR 73.100(b)(3)(i), the design of physical security SSCs relied on for interior and exterior intrusion detection functions shall provide assurance of detecting unauthorized access into vital and protected areas. The design should be redundant, independent, and diverse to ensure the reliability and availability of systems and components to achieve the intended intrusion detection functions.

A. Exterior intrusion detection—The design of physical protection SSCs relied on for exterior intrusion detection functions should be redundant, independent, and diverse to provide a detection probability of 90 percent with 95 percent confidence. There should be a minimum of two continuous lines for detecting intrusions at the outermost plant security perimeter boundary (defined as the designated boundary for initiating security response). The designer should consider including the following:

- At least two different types of sensors should provide overlapping detection within each intrusion detection zone (i.e., two continuous lines).
- Sensors should be complementary to achieve a higher probability of intrusion detection and a low nuisance alarm rate, ensure the operation of a sufficient number and diversity of sensors to maintain at least a 90 percent probability of detection during any conceivable environmental disturbance, and increase the difficulty of the task for a covert intruder attempting to defeat the system.
- Detection systems and subsystems should be capable of self-testing and monitoring of system hardware for normal and abnormal conditions, tamper protection and indication, alarm communication signal line supervision, and lighting protection.
- Alarms, communications, and display network architecture should be redundant with point-to-point connection that is bidirectional, or equivalent, to prevent a single-point failure that would disable any part of the system.
- Encryption should be provided to protect the integrity of signals between data gathering equipment and alarm computers.
- Uninterruptible power supply should provide continuity of system functions, preventing a temporary loss or disruption of system functions. Uninterruptible power should be available at least 8 hours with backup power supply capable of providing continuity of system functions for at least 24 hours.
- Access control portals located on the outermost plant security perimeter boundary should maintain intrusion detection capabilities and be capable of facilitating a timely security response.
- Digital security systems should be independent and physically isolated, or air-gapped, from other plant networks to protect against cyberattacks.
- Compensatory measures should be identified for failure of components and systems that may compromise detection effectiveness, such as weather events.

B. Interior intrusion detection—The design of physical security SSCs relied on for interior intrusion detection functions should be redundant, independent, and diverse to provide a detection

probability of 90 percent with 95 percent confidence for initiating security responses. The design should meet the criteria set forth for exterior intrusion detection systems above and, in addition, consider including the following:

- devices and equipment that meet industry standards established for listing or approval by independent testing laboratories for interior intrusion detection functions;
- devices and equipment that account for environmental conditions, including radiation and chemically corrosive environments, extreme temperatures, and the effects of these environmental conditions on the performance of interior sensors; and
- locations, configurations, and installations of intrusion detection sensors that account for vulnerabilities to insider tampering.

C. Relevant guidance—The design considerations are informed by guidance found in, but not limited to, the following:

- RG 5.44, "Perimeter Intrusion Alarm Systems."
- RG 5.76, "Physical Protection Programs at Nuclear Power Reactors," (SGI).
- NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," issued September 2017 (Ref. 36)
- NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Planning Document," issued June 1980 (Ref. 37)
- NUREG/CR-4298, "Design and Installation of Computer Systems to Meet the Requirements of 10 CFR 73.55," issued 1985 (Ref. 38)
- NUREG/CR-1468, "Design Concepts for Independent Central Alarm Station and Secondary Alarm Station Intrusion Detection Systems," issued November 1980 (Ref. 39)
- SAND2021-0543," Security System Design Reference, Intrusion Detection and Video Assessment," issued January 2021 (Ref. 40)
- J. Russell, "Complementary Sensor Selection for High Security Applications," September 2012 (Ref. 41).

4.1.1.2 Intrusion Assessment—10 CFR 73.100(b)(3)(ii)

A. Assessment—The design of physical security SSCs relied on for alarm assessment functions should be redundant, independent, and diverse to provide immediate capture of images and rapid remote assessment for determining the causes of intrusion alarms and initiating security responses. The design ensures that a single failure does not result in loss of the system's capabilities to provide rapid remote assessment and immediate capture of images. The designer should consider including the following:

- an alarm assessment system that provides increasingly diverse and overlapping closed-circuit television coverage progressing closer to the critical detection point, such as single cameras with overlapping fields of coverage on the exterior perimeter, and at least two independent and diverse cameras for each alarm zone for interior zones, so that

a single failure does not result in the loss of the capabilities to rapidly assess an alarm zone;

- dedicated physical security SSCs that are relied on for images, signal transmission, switching, system and component control, recording, and display that are redundant for communication and power failures, separated, and diverse so that a single failure does not result in loss of immediate alarm assessment functions;

- an uninterruptible power supply that prevents temporary loss of system functions and a backup power supply that provides continuity of assessment functions for at least 24 hours;

- monitoring with assessment equipment designed to provide real-time and playback/recorded video images of the detected activities before and after each alarm annunciation;

- tamper protection that includes detecting loss of and authentication of signals, line supervision, and detecting physical tampering of transmission, camera, switching, controller, and recording and display equipment;

- primary and backup lighting systems that provide sufficient ground level illumination for cameras to create images with resolution necessary for assessment (for imaging systems that do not rely on lighting, such as thermal imagers, sufficient resolution of resulting images to allow for rapid and effective assessment);

- alarm assessment controls and graphics and video displays that account for human-machine interfaces, including ergonomic and human factors, rapid assessment, alarm response, and system and component controls;

- when a licensee can use technology to assess the cause of an alarm, completion of the alarm assessment within 45 seconds, and, when an in-person (e.g., response by a security patrol) or other method (e.g., observation by a security officer who is posted in a bullet-resistant enclosure and has direct line of sight) of supplemental examination of an alarm zone is necessary, initiation of the supplemental examination within 45 seconds; and

- compensatory measures identified for the failure of components and systems that may compromise assessment effectiveness, such as weather events.

B. Relevant guidance—The design considerations are informed by guidance found in, but not limited to, the following:

- RG 5.76

- NUREG-1959

- NUREG/CR-0543

- SAND2021-0777, “Security System Design Reference, Alarm Communication and Display, and Security Communications,” issued 2021 (Ref. 42)

4.1.1.3 Security Communication—10 CFR 73.100(b)(3)(iii)

A. Communication—The design of physical security and plant SSCs relied on for onsite and offsite security communications should be redundant, independent, and diverse for continuity and integrity of communications and shall account for threats up to and including the DBT that can affect the reliability and availability of security communications. The designer should consider the following:

- combinations of diverse communication systems that account for (1) threats up to and including the DBT that can interrupt or interfere with the continuity or integrity of communications, and (2) the systems' continued function under normal and adverse conditions, severe weather, and plant emergencies;
- digital security communication systems that are independent and physically isolated, or air-gapped, from other plant networks to mitigate cyberattacks, as described in RG 5.71 or DG-5075, "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed under 10 CFR Part 53" (proposed new RG 5.96) (Ref. 43);
- an uninterruptible power supply that prevents temporary loss of system functions and a backup power supply that provides continuity of communication functions for at least 24 hours; and
- encryption that protects the integrity of communication signals.

B. Relevant guidance—The design considerations are informed by guidance found in, but not limited to, the following:

- RG 5.76
- RG 5.71
- NUREG-1959
- NUREG/CR-0543
- SAND2021-0777
- SAND99-2392, "Technology Transfer Manual—Protecting Security Communications," issued 1999 (Ref. 44)

4.1.1.4 Security Response/Neutralization—10 CFR 73.100(b)(3)(iv)

A. Onsite response—The design of engineered security SSCs relied on for neutralization functions should be redundant, independent, and diverse. Whenever possible, it should consider the design of buildings and structures to provide assurance of opportunities and capabilities to neutralize adversaries. The design shall ensure that a single failure does not result in the loss of capability to neutralize adversaries in that area or sector. Exercises should be conducted regularly for training and to validate effectiveness of the physical protection system. The design should provide defense in depth and consider the following:

- Exterior Defense: Defense in depth should be provided for neutralization functions with an exterior protection layer of at least two overlapping fields of fire covering each sector of the outermost perimeter physical barriers. The actual number of overlapping fields of

fire should be dictated by the amount of time the adversary is exposed between the time of detection and the first delay element or opportunity for the adversary to obtain cover or concealment. The shorter the timeline for the adversary to reach cover or concealment, the more overlapping fields of fire should be dedicated to that sector, increasing the probability of neutralization. Each responder should have a maximum engagement range of 200 yards for sectors covered.

- Delay: The exterior defense should be augmented by delay features to provide maximum engagement opportunities for exterior responders. These delay features may consist of distance from the time of detection to the first delay barrier or opportunity for cover or concealment, delay barriers, and reinforced or complex access control systems for entry to the reactor building and structures. Applicants and licensees should determine whether certain delay features may also provide the DBT adversary with an advantage (e.g., using obscurants without the site protective force having thermal vision equipment, installing solid vehicle barriers in such a manner as to provide an adversary with cover from site firing positions); if such an adversary advantage exists, applicants and licensees should select different delay features or modify their physical protective programs or strategies to eliminate or mitigate it.

- Interior Defense: The interior defense should provide protection inside buildings and structures for neutralization functions, covering the pathways and plant areas inside the reactor and support buildings where SSCs and equipment capable of placing radiological material in an unsafe state are located. The interior layer of protection should be designed so that a single failure does not result in the loss of capability to neutralize the adversary before task completion.

- Ballistic Protection: The ballistic resistance of engineered fighting positions should protect those performing the neutralization function. The ballistic resistance should preclude the maximum caliber, bullet weight, and bullet velocity of projectiles fired by the DBT adversary's hand-carried small arms, as described in RG 5.69, to penetrate an applicant or licensee's fighting positions.

- Blast Protection: Fully enclosed fighting positions should provide protection against overpressure for security responders to remain combat effective. Blast protection should ensure that overpressure within the fighting position does not exceed 2 pounds per square inch (psi). The design of the fighting positions should withstand blast overpressures of a maximum quantity of hand-carried explosives from a single adversary detonated at a distance of 50 feet. In addition, the configuration and construction of fighting positions should be designed so that no more than one fighting position is rendered combat ineffective due to overpressure of a person or damage to the structure from the maximum quantity of DBT vehicle-borne explosive.

- Remotely Operated Weapons Systems (ROWS): Where engineered remotely controlled weapon systems are relied on for neutralization functions, the designer should consider including the following for reliability and availability of the system's intended functions, as applicable:

    - Ballistic protection of weapons and system components from all sides is provided to protect features relied on to perform intended neutralization functions.

- Features relied on for target acquisition and weapon control are redundant, independent, and diverse such that a single failure does not result in loss of the system's ability to acquire targets or control firing of weapons.
- Features relied on for image signal transmission lines and weapon control signal lines are redundant, independent, and diverse such that a single failure, action, or inaction does not result in loss of capability to visually and mechanically acquire target and fire.
- Tamper protection includes line supervision of control and video signals and configurations and installations to protect against insider threats.
- Reliable primary and backup power and an uninterruptible power supply are provided for continuity of system functions.
- Design features are provided that account for environmental conditions that could potentially affect the performance of cameras, power supply, hydraulics, and other components of the weapon platform and ballistic protection. Such environmental conditions could include snow, fog, rain, humidity, freezing temperatures, heat, sand, pests, or other site-specific conditions.
- The design accounts for human factor and human/machine interfaces to ensure the reliability and availability of neutralization functions.
- Digital systems prevent misuse and ensure high probability of functionality and effectiveness.

B. Offsite response—The response force shall be properly trained, qualified, and equipped to interdict and neutralize threats up to and including the DBT for radiological sabotage. The design should provide defense in depth and consider the following:

- ensuring the response force has adequate knowledge of the facility and target locations to implement a proper response to a malicious act,
- ensuring the response force is adequately trained to neutralize a DBT adversary force,
- conducting exercises regularly with the response force for training and to validate the effectiveness of the physical protection system,
- ensuring the response forces arriving from offsite have adequate knowledge to respond to an adversary force that has already taken control of the site,
- developing secondary contingency routes for the response force to reach the facility and considering methods to ensure the confidentiality of response force routes to the facility, and
- if relying on law enforcement for interdiction and neutralization functions, ensuring the following actions:
  - Develop a written law enforcement response plan by the licensee that documents coordination between the licensee and law enforcement agencies (LEAs) expected to respond to the site during a contingency event.

- During the planning for law enforcement response, consider the potential impacts of the site emergency plan and the possibility of adverse impacts to the interface of safety and security in accordance with 10 CFR 73.58. RG 5.54 and DG-5072 contain further guidance regarding law enforcement responses.

DG-5072 (proposed new RG 5.90) contains further guidance associated with offsite response using a proprietary or contracted response force or LEA.

C. Security delay

- The design of physical delay systems (i.e., dedicated physical security SSCs, plant safety- or non-safety-related SSCs, and facility or site configurations that delay the DBT adversary) shall provide assurance for security response with defense in depth of opportunities to interrupt adversary tasks. The design should do the following:
  - Consider that the combination of passive and active physical barrier systems, including spatial separations, credited for delay times are only those that occur after intrusion detection; the barrier's delay times should account for uncertainties by applying the most conservative (i.e., the shortest) amount of time it would take an adversary to traverse (by motorized vehicles or on foot), penetrate (by mechanical or explosive breaching, or both), bypass over or under, or otherwise defeat physical barriers.
  - Account for the delay time needed for the most demanding (i.e., longest or slowest) security response time for reasonable assurance of security response to interrupt adversary tasks.
  - Account for the safety and security interfaces in the design to mitigate effects on manual operator actions necessary for public health and safety.
  - Demonstrate that the postulated delay for an offsite response for the facility is long enough to allow an adequately sized offsite response force to arrive in time to accomplish its interdiction and neutralization functions.
  - Consider that an offsite response would likely require a significant amount of delay after detection.
- Delay can be accomplished by physical barriers, activated delays, or responders. The task time to breach a barrier is considered a delay only if it occurs after detection with assessment and only after notification of the response force. Some deployable delay techniques can be effective, but applicants and licensees should consider their effect on site personnel (safety, security) and on the offsite response force responding after the adversary. Delay opportunities may include, but are not limited to, the following:
  - long distance between the protected area barrier and reactor and support buildings;
  - delay barriers between the protected area barrier and support structures, such as stacked razor wire sandwiched between fences;
  - limited number of entrances to buildings (considering safety and security interface);

- added delay elements to building entry systems, such as reinforced doors that anchor in place in a security event, or entry requirements (biometrics);
- internal defenders or ROWS covering all access points (where, ideally, response positions are built in, though mobile fighting positions can be effective); and
- vital area door lockout and reinforcement.

DG-5072 (proposed new RG 5.90) contains further guidance on security delays.

D. Relevant guidance—The design considerations are informed by guidance found in, but not limited to, the following:

- RG 5.76
- RG 5.54
- NUREG/CR-0543
- SAND2007-5591
- SAND2021-15454, "Security System Design Reference, Interim Access Delay," dated May 31, 2022
- SAND2011-9366, "Technology Transfer Manual—Access Delay," Volume 1, issued September 2013 (Ref. 45)
- Interagency Remotely Operated Weapon Systems (IROW)-002, "Performance Specification System Specifications for the Interagency Remotely Operated Weapon Systems (IROWS)," dated February 2009 (Ref. 46)
- SAND2013-0038, "Security-by-Design Handbook," issued 2013 (Ref. 47)
- DG-5072 (proposed new RG 5.90)

4.1.1.5 Control Measures Protecting against Land and Waterborne Vehicle Bomb Assaults—10 CFR 73.100(b)(3)(v)

A. The design of physical security SSCs and plant and facility features relied on to protect against a DBT land-borne vehicle bomb may include a combination of passive and active physical barriers and natural land barriers. Defense in depth should be incorporated from the point of the possible land-borne vehicle bomb explosion to the structures (e.g., reactor building) containing critical reactor safety SSCs by determining a minimum safe-standoff distance, using structural design, or a combination of the two to withstand blast effects, and a safe-standoff distance based on 1.5 times the maximum DBT quantity of explosives, as described in RG 5.69. Other factors to consider for passive and active vehicle barrier systems include reliability, maintainability, sabotage resistance, and probability of malfunction. The designer should consider including the following:

- The perimeter of the entire passive and active vehicle barrier system should be protected from adversary attempts to defeat and bypass passive or active vehicle barrier systems.

- Entry of private motor vehicles into secured areas should be minimized or eliminated, if possible.

- The design parameters for a passive vehicle barrier system to withstand collision of vehicles should apply conservative values for the coefficient of restitution (e) (value of 0.3) and coefficient of friction (μ) (value of 0.35 for grass covered surface and 0.45 for other surfaces (e.g., concrete, asphalt, gravel)), with a minimum barrier height and depth required to withstand a DBT adversary vehicle.

- Vehicle barrier systems and natural terrain should ensure that the DBT adversary vehicles cannot penetrate past the interior edge of a delay barrier.

- Physical barriers, and their configurations, for vehicle access control points should establish (1) an approach zone that enforces reduced speed, prescreening, queuing, and an opportunity to identify potential threat vehicles, (2) an access control zone that includes access processing and vehicle inspections, and (3) a response zone that includes a final access barrier and overwatch fighting position. The configuration should account for maximum operational vehicle traffic volume and vehicle sizes.

- The vehicle access control points should include (1) a final active vehicle barrier system and minimum distances in the response zone that provide sufficient time to deploy the active vehicle barrier system to a denied position, (2) a second active vehicle barrier system that is located between the approach zone and the access control zone, and (3) a passive physical barrier system that is continuous from the point of entry into the approach zone to termination at the final active barrier system in the response zone.

- Overwatch fighting positions observing vehicle access control points should have the same ballistic and blast-resistant protections as described in section 4.1.1.4.A to maintain the security responder's combat effectiveness.

- Engineered physical barriers, natural barriers, and any combination of engineered and natural barrier systems (for example, an adjacent body of water such as a seashore, lake, river, or stream) should account for physical changes, such as drought, low tide, and freezing of water, that may allow a land-based vehicle to bypass or defeat the intended vehicle barrier functions.

- Vehicle barrier controls should not be externally mounted and should be inside a forced-entry-rated/ballistic-rated/blast-rated enclosure such as a guard booth.

- Master vehicle barrier controls should be located at the central alarm station and be capable of overriding the entry control point vehicle barrier controls.

- Vehicle barriers should be maintained in the denial position unless being temporarily lowered by authorized personnel for vehicle entry.

- For entry control points requiring vehicle inspection before entering an area, vehicle barriers should be structured and positioned such that at least two are placed at each entry control point in succession, both in the denial position by default. Under normal conditions, vehicle barrier operators should be able to have only one barrier in the access (i.e., lowered) position at a time. Upon arrival and no apparent signs of threat, operators should lower the outermost barrier allowing for the vehicle to enter in between the barriers, and then raise the outer barrier "trapping" the vehicle and allowing for

inspection and verification of the occupants' credentials. If the vehicle is granted access after inspection and verification of credentials for occupants, the inner barrier can be lowered allowing the vehicle access to the area. The process should be accomplished in reverse for exit from the area, although verification of the occupants' credentials may not be necessary for exit depending on site-specific procedures.

- All equipment necessary for vehicle barrier operation, such as hydraulic boxes, should be installed inside the perimeter and protected against ballistic or high energy attack.
- If any components required for active vehicle barrier operation are damaged or fail, the barrier should "fail secure," remaining in the secured or denial position (i.e., damage of the vehicle barrier hydraulic boxes should not lower the barrier).
- An uninterruptible power supply should be provided to prevent temporary loss of active barrier functions for at least 24 hours.
- Facility-owned vehicles as well as construction equipment, whether permanently or temporarily located on site, should be secured to prevent malicious use.
- Vehicle barriers should satisfy testing standards such as American Society for Testing and Materials (ASTM) F 2656M-15, "Standard Test Method for Crash Testing of Vehicle Security Barriers" (Ref. 48), or International Workshop Agreement (IWA) 14-1:2013, "Vehicle Security Barriers—Part 1: Performance Requirement, Vehicle Impact Test Method and Performance Rating" (Ref. 49).
- The licensee should perform an analysis or conduct performance testing for attacks that are not part of the vehicle barrier test standard but that might be part of the adversary pathways.

B. Waterborne—The design of physical security SSCs and plant and facility features relied on to protect against the DBT waterborne vehicle bomb may include installation of active and passive engineered vehicle barriers and natural land barriers. Defense in depth should be incorporated from the point of the possible waterborne vehicle bomb explosion to the structures (e.g., reactor building) containing critical reactor safety SSCs by determining a minimum safe-standoff distance, using structural design, or a combination of the two to withstand blast effects and a safe-standoff distance based on 1.5 times the maximum DBT quantity of explosives, as described in RG 5.69. The perimeter of the passive and active vehicle barrier system should be protected through implementation of delay, detection, assessment, and interruption of adversary attempts to defeat and bypass passive or active vehicle barrier systems. Engineered physical barriers, natural land features, or a combination of engineered and natural barriers should account for changes to water level (e.g., flooding, heavy rain, high and low tides, drought conditions) that may allow waterborne vehicles to bypass or defeat the intended barrier functions.

C. Relevant guidance—The design considerations are informed by guidance found in, but not limited to, the following:

- RG 5.76
- RG 5.68, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants" (Ref. 50)
- NUREG/CR-6190

- USACE, "Update of NUREG/CR-6190 to Reflect Revised Design Basis Threat," dated March 2004 (Ref. 51)
- USACE PDC-TR-06-05, "Evaluating Adequacy of Landform Obstacles as Vehicle Barriers," dated August 2007 (Ref. 52)
- USACE PDC-TR-06-06, "Passive Inertial Vehicle Barrier Design Guide," dated August 2007 (Ref. 53)
- USACE PDC-TR-06-09

4.1.1.6 Access Control Portals—10 CFR 73.100(b)(3)(vi)

A. The design of access control portals (or entry and exit portals) and physical security SSCs relied on for controlling entry and exit for persons and material is integral to the physical barrier systems and vehicle access points to protect against threats up to and including the DBT. Redundant, independent, and diverse physical security SSCs should provide a detection probability of 90 percent with 95 percent confidence. The design should include at least two complementary and diverse means for detecting or identifying SNM, metal parts, incendiaries, explosives, and other contraband.

B. The design of access control portals and physical security SSCs relied on for denying unauthorized access to persons (including the DBT adversary) and pass-through of contraband materials (e.g., weapons, incendiaries, explosives, and other materials) or removal of SNM should include the following:

- Controls relied on to verify authorized persons entry and exit should be redundant and independent. Such controls should ensure that two unlikely, independent, and concurrent failure conditions of three entry control features (e.g., coded credential photo identification, personal identification number, and biometric verification) should occur for an unauthorized entry or exit. The design should preclude the use of a credential to enter the protected area if the credential is already assigned in the system as being inside the protected area.
- Physical barriers and configurations of the portals should separate people who are entering from people who are exiting. The portals should not permit exiting people to reenter without verification and searches. The portals should also prevent a person or materials from being able to bypass controlled verification and search areas by going above, below, or around the portal.
- When an access control portal is located on the most exterior physical barrier, the control portals delay time should be at least equivalent to the physical barrier's delay time required for security response. An automated system that controls the ability of people to enter or exit should be integrated with capabilities of physical barrier systems, such as lockdown of entry and exit openings.
- The following SSCs should be redundant, independent, and diverse to ensure reliability and availability of detection, assessment, and response functions in the face of attempted unauthorized personnel access through, or bypass of, the access control portals: intrusion detection and assessment (exterior and interior), duress alarms, tamper protection, security communications, interior and exterior lighting, uninterruptible power supply, and backup power supply.

- The design of physical security SSCs relied on for detecting unauthorized removal of SNM should be redundant, independent, and diverse to provide a detection probability of 90 percent with 95 percent confidence. There should be at least two complementary and diverse means for detecting the unauthorized removal of SNM.

- SSCs relied on for searching persons and materials to detect weapons and explosives or incendiary devices containing metal parts should be redundant, independent, and diverse to provide, at any point, a detection probability of 90 percent with 95 percent confidence. The design should include at least two complementary and diverse means for detecting or identifying metal parts.

- SSCs relied on for searching persons and materials for DBT hand-carried explosives should be redundant, independent, and diverse to provide a detection probability of 90 percent with 95 percent confidence. The design should include at least two complementary and diverse means for detecting or identifying explosives.

C. Relevant guidance. The design considerations are informed by guidance found in, but not limited to, the following:

- RG 5.76
- USACE PDC-TR-06-09
- SAND2007-5591
- SAND99-2168

4.1.1.7 Target Set Identification

Consistent with 10 CFR 73.100(b)(4) and 10 CFR 73.100(b)(5), the licensee shall identify and analyze site-specific conditions, including target sets, that may affect the physical protection program needed to implement the requirements of this section and shall identify target sets and maintain the process used to develop target sets in accordance with 10 CFR 73.55(f). As described in 10 CFR 73.55(f), each licensee shall document and maintain the process used to develop and identify target sets. The identification of target sets provides a key planning basis for the design of the site's protective strategy, and the protection of target sets should be the primary focus of armed response force personnel. RG 5.76 and DG-5071 (revised RG 5.81) provide additional guidance for the development of target sets.

4.1.1.8 Performance Evaluation Program

Consistent with 10 CFR 73.100(b)(6), each licensee shall establish, implement, and maintain a performance evaluation program (PEP). Each licensee shall establish methods appropriate and necessary to assess, test, and challenge the integration of the physical protection program's functions to protect against the DBT of radiological sabotage.

The licensee should establish the appropriate and necessary frequencies for performance evaluations, verifications, and assessments based on the importance, security significance, reliability, and availability of physical protection program functions and implementation of programs and requirements. The physical security plan should document the frequencies associated with the PEP. The licensee should periodically demonstrate that the equipment, procedures, and personnel that comprise the physical protection program are effectively integrated and coordinated to ensure that threats to the facility would be detected, assessed, interdicted, and neutralized.

The PEP is intended to provide a documented methodology for each licensee to demonstrate that its physical protection program satisfies the response requirements of 10 CFR 73.100 and to demonstrate

that the site protective strategy effectively protects against the DBT. The PEP described in 10 CFR Part 73, Appendix B, Section VI, is one acceptable method to meet 10 CFR 73.100(b)(6). RG 5.75 provides additional details regarding the PEP.

If an offsite response force or LEA provides response functions, guidance for the conduct of contingency response and LEA force-on-force exercises can be found in DG-5072, Appendix A, "Conduct of Law Enforcement Contingency Response Plan Drills," and Appendix B, "Conduct of Law Enforcement Contingency Response Force-on-Force Exercises."

4.1.1.9 Access Authorization Program

Consistent with 10 CFR 73.100(b)(7), each licensee shall establish, implement, and maintain an access authorization program in accordance with 10 CFR 73.56 and describe the program in the physical security plan. RG 5.66 contains further guidance on the implementation of the access authorization plan.

4.1.1.10 Cybersecurity Program

Consistent with 10 CFR 73.100(b)(8), each licensee shall establish, implement, and maintain a cybersecurity program in accordance with 10 CFR 73.54 or 10 CFR 73.110, "Technology-inclusive requirements for protection of digital computer and communication systems and networks," and describe the program in the cybersecurity plan. The NRC provides further guidance on the implementation of the cybersecurity program in RG 5.71 and DG-5075 (proposed new RG 5.96).

4.1.1.11 Insider Mitigation Program

Consistent with 10 CFR 73.100(b)(9), the licensee shall establish, implement, and maintain an insider mitigation program and describe the program in the physical security plan. The insider mitigation program shall monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access or unescorted access authorization to a protected or vital area. The program should also implement defense-in-depth methodologies to minimize the potential for an insider (active, passive, or both) to adversely affect, either directly or indirectly, the licensee's capability to protect against radiological sabotage, or affect the licensee's ability to respond to a safety or security event, or adversely affect the normal operation of the plant. The insider mitigation program shall integrate elements of the access authorization program, fitness-for-duty program, cybersecurity program, and physical protection program. RG 5.77 and 10 CFR 73.56(j) provide further guidance in defining and applying the need for unescorted access and unescorted access authorization to mitigate insider threats.

4.1.1.12 Corrective Action Program

Consistent with 10 CFR 73.100(b)(10), the licensee shall be able to track, trend, correct, and prevent recurrence of failures and deficiencies in the physical protection program. The program should be implemented in a manner similar to the corresponding programs deemed important to safety and operations, consistent with quality assurance criteria implemented at the facility. Findings from physical protection program reviews should be entered into a site corrective action program.

4.1.1.13 Integration of Site Plans and Procedures

Consistent with 10 CFR 73.100(b)(11), the implementation of security plans and associated procedures shall be coordinated with other onsite plans and procedures to preclude conflict during both normal and emergency conditions. To accomplish this, the licensee shall identify and resolve areas of potential conflict. Each licensee shall consider the requirements of 10 CFR 73.58 during this review. RG 5.74 contains further guidance.

4.1.2 Security Organization

Consistent with 10 CFR 73.100(c), the licensee shall establish and maintain a security organization that is designed, staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of 10 CFR 73.100. As further required in 10 CFR 73.100(c), the security organization shall include (1) a management system for maintaining and implementing security policies and procedures that provides oversight of the onsite physical protection program, (2) implementing procedures for the conduct of security operations, security design and configuration controls, maintenance, training and qualification, and contingency responses, (3) systems for approving physical protection program designs, policies, processes, and procedures and ensuring that any revisions to them satisfy the requirements of this section, and (4) retention of all analyses, assessments, calculations, and descriptions of the technical bases for meeting the performance requirements of 10 CFR 73.100(b).

The physical security plan or implementation procedures should describe or confirm the following:

4.1.2.1 The plan should give the structure of the security organization, particularly describing command and control. The physical security plan should describe the manner in which the organization is staffed, using the position titles and duty descriptions provided in NRC regulations or approved guidance. The plan should identify and define any site-specific titles or duty descriptions, including the underlying bases or rationale for why the title or duty description is important. The plan should also describe deviations from commonly used position titles and duty descriptions. The incorporation of commonly used position titles and duty descriptions, and the identification of deviations from these titles and descriptions, is intended to ensure that the physical security plan clearly describes who has the chain-of command decision-making authority and responsibility for both normal and contingency conditions. The physical security plan should impart a clear understanding of how the security organization is structured; how required duties will be performed and by whom, by title or position or both; and who will fulfill those duties. The physical security plan should describe the security organization's training and qualification curriculum, which may be the licensee's application of the approved training and qualification plan, including any deviations or amendments to that plan.

4.1.2.2 The plan should describe the management system that is responsible for the development, implementation, revision, and oversight of procedures that implement the licensee's security program, and the process for the formal approval of implementing procedures and associated revisions to those procedures. The security plan should describe and confirm that revisions to implementing procedures will be reviewed for content, completeness, and accuracy before publication, to ensure that the implementing procedures and the actions that will be taken to apply them retain regulatory integrity and, as appropriate, have been subjected to the safety and security interface requirements in 10 CFR 73.58.

4.1.2.3 The plan should include the character, content, function, control, inventory, and availability of the equipment provided to the security organization's staff for the purpose of performing assigned duties and implementing the licensee's physical protection program.

4.1.2.4 The plan should explain the structure and hierarchy of the management system that provides oversight of the onsite physical protection program. The physical security plan should provide an organization chart or diagram displaying relevant positions or titles in a command-and-control structure; describe the member of the security organization by position title and duty description, who will be available at all times to respond to a security event and direct the

activities of the physical protection program; and confirm that there will be no duty assigned to this member that would interfere with their ability to direct physical protection program functions and activities. The management structure description should include the chain of command that will be used in the event that the primary individual is incapacitated or otherwise unable to perform these duties. The physical security plan should clearly establish the hierarchical separation and functional integration between the security organization and operational organizations.

4.1.2.5 The licensee should not permit, allow, or instruct any person to perform any activity that is required for or supports the licensee's implementation of the physical protection program unless the person has been specifically trained, equipped, and qualified to perform the activity in accordance with the licensee's approved training and qualification plan.

4.1.2.6 The licensee has developed and implemented training and qualification standards and requirements for nonsecurity licensee or contract employees who are assigned to perform any duty or activity that is required for or supports the licensee's implementation of the physical protection program.

4.1.2.7 RG 5.76 and RG 5.54 provide further guidance on the security organization.

4.1.3 Search Requirements

Consistent with 10 CFR 73.100(d), the objective of the search program is to detect and prevent the introduction of firearms, explosives, incendiary devices, or other items that could be used to commit radiological sabotage. To accomplish this, the licensee shall search individuals, vehicles, and materials consistent with the physical protection program design requirements in 10 CFR 73.100(b) and the functions to be performed at each access control point or portal before granting access.

The physical security plan should describe how the licensee implements its search program. At a minimum, the physical security plan should contain the following:

4.1.3.1 The plan should discuss the implementing methodology and programmatic elements that are relied upon to ensure that the search functions are performed effectively, which may include a general discussion of how procedures will address the chosen methodology and programmatic elements. The physical security plan should discuss how the search processes ensure that all personnel, packages, and compartmented areas of a vehicle are searched; explain how the search processes ensure that all prohibited items are detected; and clearly define and identify the items to be prevented from entering the owner-controlled area (OCA) and potentially challenging the protected area or target set components.

4.1.3.2 The plan should discuss the implementing methodology and programmatic elements that are relied upon to ensure that the OCA vehicle search is conducted using equipment capable of detecting firearms, explosives, or other incendiary devices; or is conducted directly by personnel who apply visual and physical search functions; or uses a combination of detection equipment and personnel actions. The discussion should confirm that the OCA vehicle search process is conducted by not less than two persons, one of whom is armed and observes the search being conducted. The function of the armed observer is to be able to take immediate defensive action(s) in the event of an observed condition for which a response is warranted, or an observed hostile or threatening action directed against the member of the security force conducting the search. Licensee procedures should describe the use of video surveillance equipment to observe the search and the role of a third person who can summon assistance if necessary.

4.1.4 Training and Qualification Program for Licensee Security Personnel

Consistent with 10 CFR 73.100(e), the licensee shall establish and maintain a training and qualification program that ensures personnel who are responsible for the physical protection of the facility against radiological sabotage are able to effectively perform their assigned security-related job duties for implementing the requirements of this section. Conforming to RG 5.75 would be acceptable for establishing a training and qualification program under 10 CFR 73.100.

4.1.4.1 The licensee shall ensure that the personnel who are assigned duties and responsibilities required to implement the security plans, licensee response strategy, and implementing procedures meet minimum security training and qualification requirements established to ensure each individual possesses the knowledge, skills, and abilities required to effectively perform assigned duties and responsibilities.

4.1.4.2 The purpose of the security training and qualification plan is to describe how the licensee will implement the minimum training and qualification requirements at its site and to establish the site-specific training and qualifications guidelines needed to ensure that each individual is properly suited, trained, equipped, and qualified to effectively perform assigned duties and responsibilities.

4.1.4.3 Each individual assigned to perform security duties should demonstrate an ability to meet the requirements of the duties to be performed before they are assigned to perform those duties.

4.1.4.4 A security training and qualification plan should describe each security-related task to be performed. This description should clearly establish the objectives of each task, performance characteristics of each task, standards to be applied during the performance of each task, and results to be achieved by the conclusion of each task to determine and establish successful performance.

4.1.4.5 A security training and qualification plan should describe the process that will be applied to substantiate and document that each individual has performed each task successfully.

4.1.4.6 The licensee should ensure that the security training and qualification program simulates, as closely as practicable, the specific conditions under which the individual would be required to perform assigned duties and responsibilities.

4.1.4.7 A security training and qualification plan should describe the process for identifying and accounting for site-specific conditions and changes thereto that will form the basis for determining the specific actions, duties, and responsibilities required to sustain the effectiveness of the physical protection program.

4.1.4.8 A security training and qualification plan should describe the process for ensuring that tasks performed to satisfy a training criterion or goal are performed commensurate with the conditions under which these task actions will be performed while implementing the licensee's security program and protective strategy.

4.1.4.9 The licensee should describe how the security training and qualification plan was developed and the basis for the claim that the security training program ensures that the personnel responsible for physical protection of the facility against radiological sabotage are able to effectively perform their assigned security functions.

4.1.4.10 With regard to the training and qualification program for law enforcement responders, if relying on law enforcement responders to fulfill the interdiction and neutralization functions, the licensee should demonstrate that site-specific training and drills have been conducted to familiarize the law enforcement responders with the site sufficiently to fulfill their duties. DG-5072 (proposed new RG 5.90) contains further guidance on reliance on law enforcement responders to perform the interdiction and neutralization.

4.1.5 Security Reviews

4.1.5.1 A critical aspect of any program is a method to evaluate its effectiveness and the continued applicability of specific program elements. The evaluation process, a proactive approach for assessing, evaluating, and improving the physical protection program, can be used as a basis for further development and improvement. Program reviews shall be designed to ensure that the physical protection program maintains effectiveness and meets requirements.

4.1.5.2 When a review is conducted following a change to personnel, procedures, equipment, or facilities that could adversely affect security, the scope of the review may be limited to those affected elements.

4.1.5.3 Physical protection program reviews shall consider the effectiveness of each component in performing its intended function within the physical protection program to ensure that the capability to detect, assess, interdict, and neutralize the DBT of radiological sabotage is maintained. Licensees may use the results of security physical protection program reviews to identify the need for improvements or program changes to ensure program effectiveness.

4.1.5.4 Consistent with 10 CFR 73.100(f), individuals independent of licensee management and personnel who have direct responsibility for implementing the physical protection program shall conduct the security program reviews. The licensee should select personnel who have sufficient site-specific and programmatic knowledge and experience in the program area to which they are assigned.

4.1.5.5 Consistent with 10 CFR 73.100(f)(3), reviews of the security program shall include, but not be limited to, an audit of the effectiveness of the physical protection program; security plans; implementing procedures; cybersecurity programs; safety and security interface activities; the testing, maintenance, and calibration program; and response commitments by local, State, and Federal law enforcement authorities.

4.1.5.6 Consistent with 10 CFR 73.100(f)(4), a report shall document the results and recommendations of the onsite physical protection program review of management's findings regarding program effectiveness and any actions taken as a result of recommendations from prior program reviews.

4.1.5.7 Consistent with 10 CFR 73.100(f)(4), all reports of such reviews shall be maintained in auditable form and made available for inspection upon the request of an authorized NRC representative. Records retention requirements appear in 10 CFR 73.100(j).

4.1.6 Performance Evaluation

Consistent with 10 CFR 73.100(g), licensees shall include methods appropriate and necessary to assess, test, and challenge the integration of the physical protection program's functions to protect against the DBT of radiological sabotage. Section 4.1.1.9 of this document provides guidance to establish,

implement, and maintain a PEP. RG 5.75 and DG-5072 (proposed new RG 5.90) contain further guidance on an acceptable method to meet this requirement.

4.1.7 Maintenance, Testing, Calibration, and Corrective Actions

Consistent with 10 CFR 73.100(h), the licensee shall ensure that security SSCs, including supporting systems, are inspected, tested, and calibrated for operability and performance at intervals necessary and sufficient to meet the requirements of 10 CFR 73.100.

4.1.7.1 Licensees should perform operability testing of intrusion detection and assessment SSCs before they are placed into service, before they are taken out of service for routine maintenance, and at least every 7 days during continuous use. Performance testing against applicable defeat methods should be conducted at least semiannually (e.g., running, walking, crawling, rolling, bridging, jumping, climbing, tunneling).

4.1.7.2 Equipment required for security contingency response communications, including with law enforcement or other offsite responders, if they are relied on for DBT adversary interdiction and neutralization, should be tested for operability at least at the beginning of each security personnel work shift. Equipment required to communicate between the alarm station(s) and control room(s), and between the alarm station(s) and local LEAs, to include backup communications equipment, should be tested for operability at least once each day.

4.1.7.3 Search and SNM detection equipment should be tested for operability at least once each day and tested for performance at least once during each 7-day period.

4.1.7.4 Active and passive vehicle barrier maintenance should be performed in accordance with the manufacturers' specifications. Active and passive vehicle barrier inspections should be consistent with the guidance contained in USACE PDC-TR-06-03, "Vehicle Barrier Maintenance Guidance," dated February 24, 2007 (Ref. 54).

4.1.7.5 Licensee security force weapons, accessories (e.g., magazines, sights and sighting systems, holsters, and weapons racks), and ammunition should be maintained, inspected, and tested for function and accuracy in accordance with the firearm maintenance program guidance in RG 5.75.

4.1.7.6 The licensee shall implement corrective actions to ensure resolution of identified vulnerabilities and deficiencies to meet the requirements in 10 CFR 73.100.

4.1.7.7 The licensee shall establish and implement timely compensatory measures for degraded or inoperable security SSCs to meet the requirements in 10 CFR 73.100. Compensatory measures shall provide a level of protection that is equivalent to the protection that was provided before the degradation or inoperability of the security systems, equipment, or components.

4.1.7.8 The licensee shall document processes and procedures and maintain records for implementing the corrective actions; compensatory measures; and maintenance, inspection, testing, and calibration of security SSCs.

4.1.7.9 RG 5.76 contains further guidance on maintenance, testing, calibration, and corrective actions.

4.1.8 Suspension of Security Measures

Consistent with 10 CFR 73.100(i), the licensee may suspend implementation of affected requirements of this section in accordance with 10 CFR 53.740(h) under the following conditions: (1) in an emergency, when action is immediately needed to protect public health and safety, and (2) during severe weather, when the suspension of affected security measures is immediately needed to protect the health and safety of personnel.

4.1.8.1 Suspended security measures shall be reinstated as soon as conditions permit (10 CFR 73.100(i)(2)).

4.1.8.2 The suspension of security measures shall be reported and documented in accordance with the provisions of 10 CFR 73.71 or 10 CFR 73.100(i)(3). RG 5.76 contains further guidance.

4.1.9 Records

Consistent with 10 CFR 73.100(j), (1) the Commission may inspect, copy, retain, and remove all reports, records, and documents required to be kept by Commission regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor, (2) the licensee shall maintain all records required to be kept by Commission regulations, orders, or license conditions, until the Commission terminates the license for which the records were developed and shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission, (3) if a contracted security force is used to implement the onsite physical protection program, the licensee's written agreement with the contractor shall be retained by the licensee as a record for the duration of the contract, and (4) review and audit reports shall be available for inspection, for a period of 3 years. RG 5.76 contains further guidance.

D. IMPLEMENTATION

The NRC staff may use this regulatory guide as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this regulatory guide to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 53.1590, or 10 CFR 53.6090, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests" (Ref. 55), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 53, Subparts H or R, "Licenses, Certifications, and Approvals." The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

REFERENCES[2]

1. *U.S. Code of Federal Regulations* (CFR), "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Reactors," Part 53, Chapter I, Title 10, "Energy."

2. CFR, "Physical Protection of Plants and Materials," Part 73, Chapter I, Title 10, "Energy."

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

4. NRC, RG 5.44, "Perimeter Intrusion Alarm Systems," Washington, DC.

5. NRC, RG 5.54, "Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants (SGI)," Washington, DC. **(Safeguards information (SGI), not publicly available)**

6. NRC, RG 5.66, "Access Authorization Program for Nuclear Power Plants," Washington, DC.

7. NRC, RG 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements (SGI)," Washington, DC. **(SGI, not publicly available)**

8. NRC, RG 5.71, "Cyber Security Programs for Nuclear Power Reactors," Washington, DC.

9. NRC, RG 5.74, "Managing the Safety/Security Interface," Washington, DC.

2 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public website at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html. The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, Maryland. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or email pdr.resource@nrc.gov.

Copies of International Atomic Energy Agency (IAEA) documents may be obtained through its website at WWW.IAEA.Org/ or by writing the International Atomic Energy Agency, P.O. Box 100, Wagramer Strasse 5, A-1400 Vienna, Austria; telephone (+431) 2600-0; fax (+431) 2600-7; or email at official.mail@IAEA.org.

Reports authored by Sandia National Laboratories can be obtained through the Sandia Publications Database, available at http://sandia.prod.acquia-sites.com, or by contacting Sandia National Laboratories, P.O. Box 5800, Albuquerque, NM 87185.

Reports authored by the US Army Corps of Engineers are available at https://www.nwo.usace.army.mil/About/Centers-of-Expertise/Protective-Design-Center/PDC-Library/.

Reports authored by World Institute for Nuclear Security (WINS) are available at https://www.wins.org/knowledge-centre, or by contacting WINS, Landstrasser Hauptstrasse 1/18, 1030 Vienna, Austria.

International Organization for Standardization (ISO) Standards, e.g., IWA reports, are available at https://www.iso.org/standards.html.

Reports authored by ASTM are available at https://www.astm.org/, or by contacting ASTM Headquarters, 100 Barr Harbor Drive, P.O. Box C700, West Conshohocken, PA., 19428.

10. NRC, RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities," Washington, DC.

11. NRC, RG 5.76, "Physical Protection Programs at Nuclear Power Reactors (SGI)," Washington, DC. **(SGI, not publicly available)**

12. NRC, RG 5.77, "Insider Mitigation Program," Washington, DC.

13. NRC, DG-5071 (revised RG 5.81), "Target Set Identification and Development for Nuclear Power Reactors," Washington, DC, December 2019. **(Official Use Only—Security-Related Information, not publicly available)**

14. NRC, DG-5072 (proposed new RG 5.90), "Guidance for Alternative Physical Security Requirements for Modular Reactors and Non-Light-Water Reactors," Washington, DC.

15. NRC, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Washington, DC.

16. CFR, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter I, Title 10, "Energy."

17. CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter I, Title 10, "Energy."

18. NRC, NUREG/CR-7145, "Nuclear Power Plant Security Assessment Guide," Washington, DC, April 2013.

19. NRC, NUREG-1964, "Access Control Systems: Technical Information for NRC Licensees," Washington, DC, April 2011.

20. NRC, NUREG/CR-7201, "Characterizing Explosive Effects on Underground Structures," Washington, DC, September 2015.

21. NRC, NUREG/CR-6190, Revision 1, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants," Volume 1, "Vehicle Barrier System Siting Guidance for Blast Protection," and Volume 2, "Vehicle Barrier System Selection Guidance," Washington, DC, December 1994.

22. U.S. Department of Energy (DOE), Sandia National Laboratories, SAND2001-2168, "Technology Transfer Manual—Access Delay Technology, Volume 1," Albuquerque, New Mexico, 2001.

23. DOE, Sandia National Laboratories, SAND2008-5644, "Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants," Albuquerque, New Mexico, 2008.

24. DOE, Sandia National Laboratories, SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," Albuquerque, New Mexico, 2007, (ML072620172).

25. NRC, "Nuclear Regulatory Commission International Policy Statement," *Federal Register*, Vol. 79, No. 132, July 10, 2014, pp. 39415–39418.

26. NRC, Management Directive (MD) 6.6, "Regulatory Guides," Washington, DC, July 19, 2022.

27. International Atomic Energy Agency (IAEA), Nuclear Security Series No. 27-G, "Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)," Vienna, Austria, 2018.

28. IAEA, Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," Vienna, Austria, 2011.

29. IAEA, Nuclear Security Series No. 40-T, "Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities," Vienna, Austria, 2021.

30. U.S. Army Corps of Engineers (USACE) PDC-TR 06-09, "Vehicle Access Control Point Guidance," 2008, Washington, DC, ML083290217.

31. DOE, Sandia National Laboratories, SAND2000-2142, "Technology Transfer Manual—Entry Control and Contraband Detection System," Albuquerque, New Mexico, 2000.

32. DOE, Sandia National Laboratories, SAND2021-13779 R, "U.S. Domestic Microreactor Security-by-Design," Albuquerque, New Mexico, 2021.

33. DOE, Sandia National Laboratories, SAND2021-13122 R, "U.S. Domestic Pebble Bed Reactor: Security-by-Design," Albuquerque, New Mexico, 2021.

34. World Institute for Nuclear Security (WINS), Security of Advanced Reactors, Special Report Series, "Secure by Design: Guidance document principles and methods," Vienna, Austria, 2020.

35. NRC, DG-5074 (proposed new RG 5.90), "Access Authorization Program for Commercial Nuclear Plants," Washington, DC, ML22199A246.

36. NRC, NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," Washington, DC, September 2017.

37. NRC, NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Planning Document," Washington, DC, June 1980.

38. NRC, NUREG/CR-4298, "Design and Installation of Computer Systems to Meet the Requirements of 10 CFR 73.55," Washington, DC 1985.

39. NRC, NUREG/CR-1468, "Design Concepts for Independent Central Alarm Station and Secondary Alarm Station Intrusion Detection Systems," Washington, DC, November 1980.

40. DOE, Sandia National Laboratories, SAND2021-0543, "Security System Design Reference, Intrusion Detection and Video Assessment," Albuquerque, New Mexico. **(Classified report, not publicly available)**

41. Russell, John L., SAND2012-4601C, "Complementary Sensor Selection for High Security Applications," Sandia National Laboratories, Orlando, Florida, September 2012.

42. DOE, Sandia National Laboratories, SAND2021-0777, "Security System Design Reference Alarm Communication and Display, and Security Communications," Albuquerque, New Mexico, 2021. **(Classified report, not publicly available)**

43. NRC, DG-5075 (proposed new RG 5.96), "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53," Washington, DC, ML22199A257.

44. DOE, Sandia National Laboratories, SAND99-2392, "Technology Transfer Manual—Protecting Security Communications," Albuquerque, New Mexico, 1999.

45. DOE, Sandia National Laboratories, SAND2011-9366, "Technology Transfer Manual—Access Delay, Volume 1" Albuquerque, NM, printed 2013.

46. IROW-002, "Performance Specification System Specifications for the Interagency Remotely Operated Weapon Systems (IROWS)." **(Classified report, not publicly available)**

47. DOE, Sandia National Laboratories, SAND2013-0038, "Security-by-Design Handbook," Albuquerque, New Mexico, 2013. **(Classified report, not publicly available)**

48. American Society for Testing and Materials (ASTM), F2656/F2656M-15, "Standard Test Method for Crash Testing of Vehicle Security Barriers," Washington, DC, 2015.[48]

49. International Workshop Agreement, IWA 14-1:2013, "Vehicle Security Barriers—Part 1: Performance Requirement, Vehicle Impact Test Method and Performance Rating," Washington, DC, 2013.

50. NRC, RG 5.68, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants," Washington, DC.

51. USACE, "Update of NUREG/CR-6190 to Reflect Revised Design Basis Threat," Washington, DC. **(not publicly available)**

52. USACE PDC-TR-06-05, "Evaluating Adequacy of Landform Obstacles as Vehicle Barriers," Washington, DC, 2007. **(not publicly available)**

53. USACE PDC-TR-06-06, "Passive Inertial Vehicle Barrier Design Guide," Washington, DC. **(not publicly available)**

54. USACE PDC-TR-06-03, "Vehicle Barrier Maintenance Guidance," Washington, DC, February 24, 2007.

55. NRC, MD 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," Washington, DC, September 20, 2019.