U.S. NUCLEAR REGULATORY COMMISSION

REGULATORY GUIDE 5.97, REVISION 0

Issue Date: March 2026
Technical Leads: Stacy Prasad and Lou Cubellis

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).

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 53.210, "Safety criteria for design-basis accidents," requires that design-basis accidents (DBAs) demonstrate that an individual located at any point on the boundary of the exclusion area for any 2 hour period following the onset of the postulated fission product release would not receive a radiation dose in excess of 25 rem (250 millisieverts) total effective dose equivalent (TEDE); and an individual located at any point on the outer boundary of the low-population zone who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its

---

Written suggestions regarding this guide or development of new guides may be submitted through the NRC's public Web site in the NRC Library at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html, under Document Collections, in Regulatory Guides, at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/contactus.html. During the development process of new guides suggestions should be submitted within the comment period for immediate consideration. Suggestions received outside of the comment period will be considered if practical to do so or may be considered for future updates.

Electronic copies of this RG, previous versions of RGs, and other recently issued guides are also available through the NRC's public Web site in the NRC Library at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html, under Document Collections, in Regulatory Guides. This 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 ADAMS Accession No. ML25232A009. The regulatory analysis may be found in ADAMS under Accession No. ML26042A230. The associated draft regulatory guide (DG)-5076, Revision 0, may be found in ADAMS under Accession No. ML22203A131. The staff responses to the public comments on DG-5076 may be found under ADAMS Accession No. ML26042A228.

passage) would not receive a radiation dose in excess of 25 rem (250 millisieverts) TEDE.

- 10 CFR 53.620, "Manufacturing," requires security programs for any manufacturing license (ML) authorizing possession of a manufactured reactor into which fuel has been loaded at the manufacturing facility.

- 10 CFR 53.860, "Security programs," requires that each nuclear power reactor licensee or applicant under 10 CFR Part 53 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 73.54, "Protection of digital computer and communication systems and networks," establishes the requirements for cybersecurity at operating power reactors and combined license applicants.

  - 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 73.110, "Technology inclusive requirements for protection of digital computer and communication systems and networks," requires licensees to demonstrate protection against cyberattacks in a manner that is commensurate with the potential consequences from those attacks, without prescribing the specific methods that must be used to demonstrate protection.

- 10 CFR 73.120, "Access authorization program for commercial nuclear 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 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 73.100(b)(4)(i), and 10 CFR 73.100(b)(4)(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.

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.

- 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 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).

- RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors," Revision 2, (Ref. 13), describes methods that the NRC staff considers acceptable for meeting the requirements of 10 CFR 73.100(b)(5) 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 the release of radionuclides from any source from exceeding the dose reference values defined in 10 CFR 53.210. Note that RG 5.81 is designated as Official Use Only—Security-Related Information and is, therefore, not publicly available.

- RG 5.96, "Establishing Cybersecurity Programs for Commercial Nuclear Plants licensed under 10 CFR part 53" (Ref. 14), provides an acceptable method that applicants and licensees may use for establishing, implementing, and maintaining a cybersecurity program at commercial nuclear plants that are licensed under 10 CFR Part 53 subject to the requirements in 10 CFR 73.110.

- 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, combined license (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.

- International Atomic Energy Agency (IAEA), Nuclear Security Series No. 8-G, "Preventive and Protective Measures Against Insider Threats," Revision 1 (Ref. 25), describes methods and approaches for selecting, implementing and evaluating measures for addressing insider threats.

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 3150-0274 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 reviewer at: OMB Office of Information and Regulatory Affairs, (3150-0274 and 3150-0002), 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 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 53.860(a)(2) to demonstrate compliance with the provisions set forth in either 10 CFR 73.55 or 10 CFR 73.100 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.

This guidance also describes methods the NRC staff deems acceptable to demonstrate compliance with 10 CFR 53.860(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.

This document does not provide guidance to implement 10 CFR 73.55, however, 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. 26) and Management Directive and Handbook 6.6, "Regulatory Guides" (Ref. 27).

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. 28)

- 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. 29)

- 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. 30)

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))

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.

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:

- incorporating security goals into the design of engineered safety systems and operational programs to potentially reduce vulnerabilities or increase resistance to threats up to and including the DBT of radiological sabotage and utilize safety capabilities to prevent or mitigate consequences from adversary actions;

- 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, "Managing the Safety/Security Interface," (Ref. 9)
- U.S. Army Corps of Engineers (USACE) Protective Design Center Technical Report PDC-TR-06-09, "Vehicle Access Control Point Guidance," issued 2008 (Ref. 31)
- SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," issued 2007 (Ref. 24)
- SAND2000-2142, "Technology Transfer Manual—Entry Control and Contraband Detection System," issued 2000 (Ref. 32)
- SAND2021-13779 R, "U.S. Domestic Microreactor Security-by-Design," issued 2021 (Ref. 33)
- SAND2021-13122 R, "U.S. Domestic Pebble Bed Reactor: Security-by-Design," issued 2021 (Ref. 34)
- World Institute for Nuclear Security, Security of Advanced Reactors, Special Report Series, "Secure by Design: Guidance document principles and methods," issued 2020 (Ref. 35)

2. Security Operations Program—10 CFR 53.860

A commercial nuclear plant licensee under 10 CFR Part 53 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. 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. 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. 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, RGs 5.54, 5.69, 5.71, 5.75, and RG 5.76.

3. 10 CFR 73.100—Performance-Based Framework

10 CFR 73.100 outlines a graded approach to physical security, with requirements varying based on achievability of target sets, as specified in sections (a)(1)(i-iii). Regardless of how a licensee implements 10 CFR 73.100(a)(1)(i)(ii), or (iii), it must ensure that fitness for duty, access authorization, cybersecurity, and information security programs are implemented according to the requirements of 10 CFR 53.860. In addition, the licensee must implement security requirements, in accordance with 10 CFR 53.860(a)(1), 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.

10 CFR 73.100(a)(1)(i) – No Achievable Target Sets – No Active Measures Credited

When a licensee determines that a nuclear power reactor facility has no achievable target sets, the requirement in 10 CFR 73.100(a)(1)(i) relieves the licensee from the remaining requirements in 10 CFR 73.100 when the licensee does **not** credit any active measure(s) to make that determination. Relying on any active measure(s) would prevent a licensee from being relieved from the 10 CFR 73.100 requirements. Examples of active measures include, and are not limited to:

- active measures credited in a site-specific target set analysis (refer to RG 5.81, Revision 2 for guidance on target set identification), including:
    - any operator action (an action that occurs before an adversary interference precluded time), including manually reducing, or initiating the reduction of, reactor power level, and
    - any mitigative action (an action that occurs after an adversary interference precluded time), including implementing any diverse and flexible coping strategies to prevent a release from exceeding the dose reference values defined in § 53.210 (e.g., deploying portable pumps, generators, batteries, or other supporting equipment to maintain or restore key safety functions).
- active physical security measures, including:
    - any intrusion detection- or assessment-related action
    - any delay-, interdiction- or neutralization-related action, including:
        - locally or remotely locking one or more facility access points,
        - locally or remotely deploying delay a feature, such as:
            - Moving active physical barriers into the denial position
            - Dispensing chemical irritants, sticky foam, slippery gel, cold smoke, etc.
            - Activating an acoustic, directed energy, or other active denial system
        - remotely operated weapons systems (ROWS), regardless of whether they are human-controlled or autonomous

10 CFR 73.100(a)(1)(ii) – No Achievable Target Sets – Active Measures Credited

When a licensee determines that a nuclear power reactor facility has no achievable target sets based on the crediting of one or more active measures (refer to preceding paragraph), the licensee is required by 10 CFR 73.100(a)(1)(ii) to implement the requirements in 10 CFR 73.100 to the extent that the physical protection program provides reasonable assurance that the active measure(s) will be accomplished as credited. The licensee must document in its facility security plans which requirements it needs to satisfy, describe how its physical protection program satisfies those requirements, and implement the physical protection program before fuel is initially loaded into a reactor, or for a fueled manufactured reactor, before initiating the removal of the features that are required by 10 CFR 53.620(d)(1) to prevent criticality.

The scenarios below outline what physical protection elements may be necessary based on different active security measures a licensee can credit to demonstrate that no achievable target sets exist in accordance with 10 CFR 73.100(a)(1)(ii).

Scenario 1: A reactor operator performs a rapid power reduction when notified of confirmed security-initiated event. After power is reduced, no adversary actions can result in an offsite radiological release that exceeds the dose reference values defined in 10 CFR 53.210. If the licensee relies on intrusion detection and assessment systems to provide the reactor operator with sufficient time to reduce reactor power, the licensee would need to meet only some of the physical protection program elements required by 10 CFR 73.100. For example, the licensee would need to meet the requirements in, but not limited to:

- 10 CFR 73.100(b)(4)(i) and (ii) to ensure there is reasonable assurance that the intrusion detection and assessment equipment will perform the functions the reactor operator relies on within the context of threats up to and including the design basis threat of radiological sabotage;

- 10 CFR 73.100(b)(4)(iii) to enable the intrusion detection and assessment system(s) to communicate with the alarm assessor, the alarm assessor to communicate with the reactor operator (if they're different people), and the reactor operator to communicate with the reactor control system;

- 10 CFR 73.100(b)(6) to determine the extent to which the requirements in 10 CFR 73.100 apply;

- 10 CFR 73.100(b)(10) to provide reasonable assurance that the alarm monitor and reactor operator are not active insiders and will perform the action(s) the licensee expects, consistent with the timing that the licensee expects;

- 10 CFR 73.100(e), "*Training and qualification program*," might be tailored to account only for the intrusion alarm and assessment monitoring staff and their duties associated with intrusion detection, assessment, and communication; and

- 10 CFR 73.100(h) to provide reasonable assurance that the intrusion detection and assessment system(s) and the reactor control system are reliable and available.

In addition to needing to only partially implement the 10 CFR 73.100 requirements, the licensee may be exempt from certain requirements in 10 CFR 73.100, such as 10 CFR 73.100(b)(4)(iv), "Security response." In this scenario, the licensee would not be relying on the delay, interdiction, or neutralization of threats up to and including the DBT to maintain offsite radiological consequences within acceptable limits. Therefore, the licensee would not need to have armed response to perform those security functions.

Scenario 2: After a target set is lost, and after an adversary interference precluded time (AIPT) calculated in accordance with appendix C of this RG, a licensee takes mitigative action to prevent an offsite radiological release from exceeding the dose reference values defined in 10 CFR 53.210. If the licensee relies on intrusion detection and assessment systems, and an onsite or offsite armed security response to preclude adversary interference and allow the necessary mitigative actions to be performed, the licensee must comply with the physical protection program elements for those program elements. For example, consistent with the requirements in 10 CFR 73.100(b)(4)(iv)(A)(*3*) or 10 CFR 73.100(e) and 73.100(g), a licensee will need to conduct force-on-force (FOF) exercises and armed response training to verify the continued accuracy of the analyzed AIPT, since AIPT is a critical element in demonstrating regulatory compliance with 10 CFR 73.100(a)(1)(ii) in this scenario. Exercise scenarios should be run to verify AIPT, not demonstrate target set protection. The licensee should consider the following guidance when conducting exercises.

- These exercises should use target sets screened as unachievable (based on AIPT and mitigative actions) as the mock adversary's objective, starting with the target set that that was used to identify the AIPT that the licensee used to screen its target sets (i.e., the target set with the longest AIPT, aka the bounding AIPT).

- Licensees should then periodically rotate through other screened target sets to avoid repetitive training and ensure comprehensive preparedness in subsequent exercises and training to lessen the likelihood of negative training of the armed response force through repetition of a single response mission.

- Once all screened sets are used, a licensee should randomly rotate them for future exercises.

- Licensees do not need to demonstrate mitigative actions during FOF exercises because those actions are considered credible if they meet the criteria outlined in Revision 2 to RG 5.81.

10 CFR 73.100(a)(1)(iii) – Achievable Target Sets

Consistent with 10 CFR 73.100(a)(1)(iii), when a reactor facility has achievable target sets, the licensee must develop, implement, and maintain a physical protection program and use the facility security plans to fully implement the requirements of 10 CFR 73.100. 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. A licensee's security plans and physical protection program must comply with 10 CFR 73.100 before fuel is initially loaded into a reactor, or for a fueled manufactured reactor, before initiating the removal of the features that are required by 10 CFR 53.620(d)(1) to prevent criticality.

4. General Performance Objective and Requirements

As described in 10 CFR 73.100(b)(1), (2), and (3), 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; (2) defense in depth is provided in achieving performance requirements through the integration of engineered systems, administrative controls, and management measures; and (3) the physical protection program is designed to prevent the release of radionuclides from any source from exceeding the dose reference values defined in 10 CFR 53.210.

Physical security SSCs should 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)(4), 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.

A. Alarm Stations—The licensee should have two locations (e.g., alarm stations) that are continually staffed and have the same functional capabilities, whether on-site or off-site, to meet the applicable requirements in 10 CFR 73.100(b)(4)(i-iv). The licensee should identify the required security functions of an alarms station for implementing the physical protection program and meeting the applicable requirements. An alarm station should be capable of performing the following alarm station functions:

- Receiving and monitoring signals for intrusion detection,
- Receiving and monitoring video image signals to assess intrusion,
- Provide command and control of the licensee security response,
- Summoning offsite local, state, and federal law enforcement (LE) assistance, and
- Communicating with onsite/offsite security to assist implementing the security response.

Where a licensee has designed its physical protection program to include remote capabilities to control access, activate delay barriers, or operate a security interdiction/neutralization system, the design of the offsite secondary alarm station should include the systems and components for assuring reliable remote operation and control of access, delay barriers, and security systems.

If a licensee designs an alarm station to serve more than one plant site (i.e., supports the implementation of multiple physical protection programs), the alarm station should be equipped and sufficiently staffed to provide the capability of monitoring and responding to multiple alarms, performing simultaneous assessments, initiating multiple security systems responses, providing command and control of the responses, and summoning for offsite assistance for all serviced sites.

4.1 Performance Requirements

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

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

A. Exterior intrusion detection—Consistent with the guidance in RG 5.44, 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 allowing 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 5.12, "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."

- RG 5.76, "Physical Protection Programs at Nuclear Power Reactors," (SGI) (Ref 11.).

- NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," issued September 2017 (Ref. 36)

- NUREG-1964, "Access Control Systems," issued April 2011.

- 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).

4.1.2 Intrusion Assessment—10 CFR 73.100(b)(4)(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 diverse and overlapping closed-circuit television coverage progressing prior to or at 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:

- NUREG-1959

- RG 5.76, “Physical Protection Programs at Nuclear Power Reactors,” (SGI) (Ref 11)

- NUREG/CR-0543

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

4.1.3 Security Communication—10 CFR 73.100(b)(4)(iii)

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 must 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 RG 5.96;

- 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.

A. Communication with law enforcement (LE) agencies or other offsite armed responders—Licensees should coordinate with LE or other offsite armed responders (e.g., licensee proprietary or contracted force) to identify communications systems capabilities that will be available during a security contingency response and ensure that offsite responders clearly understand whether their radio frequencies are integrated into the facility's infrastructure (e.g., a facility's radio frequency repeaters are the correct band and are programmed with LE radio frequencies) and any limitations that may exist (e.g., radio frequency dead zones).

Licensees should provide relevant satellite and cellular phone lists for important site locations or functions (e.g., alarm stations, control room), as well as direct dialing instructions to or from any licensee satellite phones. Licensees should consider the following example for how to provide this information to LE or other offsite responders:

Example: Satellite Information

[Facility name] has [insert number] satellite phones in service during a typical day, [insert number] of which are located inside the protected area. The facility also has the capability to employ additional [insert number] satellite phones (aka FLEX satellite phones); however, LE needs to be aware the FLEX satellite phones are not immediately available to on-duty site personnel and may not be in service when LE responders arrive at the facility. Table 1 below lists the satellite phone numbers and their assigned locations.

[Insert general descriptor (e.g., some, most) or specific number] of the facility's satellite phones have 10-digit U.S. phone numbers, but [insert number] of them have 12-digit international numbers. To place calls to or from the facility's satellite phones, use these dialing instructions:

<u>Dialing instructions for the satellite phones with 10-digit U.S. phone numbers</u>:

- To satellite phone from landline or cell phone, dial 1 + phone's 10-digit number
- From satellite phone to landline or cell phone, dial 1 + phone's 10-digit number
- From satellite phone to another satellite phone, dial 001 + 10-digit phone number

Dialing instructions for the satellite phones with 12-digit international numbers:

- To satellite phone from landline or cell phone, dial 011 + 12-digit satellite phone number
- From satellite phone to landline or cell phone, dial 001 + area code and phone number
- From satellite phone to another satellite phone, dial 00 + 12-digit satellite phone number

Table 1. [Facility name] Satellite Phone Information

Satellite Phone Location	Satellite Phone Number
Control Room*	(xxx) xxx-xxxx
Control Room*	(xxx) xxx-xxxx
FLEX Building	xxxx xxxx xxxx
Work Execution Center	xxxx xxxx xxxx

* Location is inside the Protected Area.

B. Offsite Alarm Station Communication—Offsite alarm stations should consider the design for communications where the SSCs' dedicated or plant operations systems relied on for communications provide assurance of continuity and integrity of alarms, video, voice, and text, and where applicable, instrument and control communications between the secondary alarm station and the site and LE agencies or other offsite armed responders.

- Protection of safeguards information and other sensitive signal transmissions:
    - Some communications or data that are transmitted between a site and an offsite alarm station (aka 'data in motion' or 'data in transit') could contain safeguards information (SGI). Licensees should adequately protect SGI in such circumstances using appropriate security controls and technologies, such as those supporting communications using data encryption, to prevent unauthorized access to SGI. Consistent with 10 CFR 73.22(f)(3), licensees should use data encryption that complies with Federal Information Processing Standard (FIPS) 140-2, "Security Requirements for Cryptographic Modules," (Ref. 43) or a subsequent revision to FIPS 140-2, i.e., FIPS 140-3, "Security Requirements for Cryptographic Modules," (Ref. 44).
    - Licensees should ensure that other sensitive signals being transmitted intermittently or continuously between a facility and an offsite secondary alarm station are adequately protected. Such signals may not meet the definition of SGI, but they may be critical for a licensee to meet the performance objective and requirements in 10 CFR 73.100(b). Examples of important signals include, but are not limited to, those that relate to access control; intrusion detection and assessment; command and control; and controls for delay, interdiction, and neutralization measures. Sensitive signals need to be adequately protected from threats up to and including the DBT, so that the associated security equipment will perform its designed function(s) and a licensee can satisfy the capabilities required by 10 CFR 73.100(b)(4)(i-iv)).

- Licensees can refer to the following guidance related to equipment used to transmit SGI or other sensitive signals:

- RG 5.74, and other relevant publications, including:
- Revision 2 to National Institute of Standards and Technology (NIST) Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations" (Ref. 45),
- Revision 5 to NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations" (Ref. 46), and
- Revision 3 to NIST Special Publication 800-82, "Guide to Operational Technology (OT) Security" (Ref. 47).

- A licensee may use a monitoring service to fulfill the security functions that should be performed by a secondary alarm station.
  - The monitoring service should be certified by an independent testing and certifying organization promulgating for such services to ensure that the service is reliable, available, and capable of implementing the licensee's physical protection program that is designed to meet the objectives and requirements of 10 CFR 73.100(b).
- Licensees should establish, implement, maintain, and document communications that are necessary to facilitate an effective response by LE or other offsite armed responders, including the use of special signals. Examples include, but are not limited to primary and secondary radio frequencies and verbal and non-verbal fratricide mitigation measures (aka identify-friend-or-foe (IFF) measures).

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

- RG 5.75
- RG 5.76, "Physical Protection Programs at Nuclear Power Reactors," (SGI) (Ref 11)
- RG 5.71
- NUREG-1959
- NUREG/CR-0543
- SAND2021-0777
- SAND99-2392, "Technology Transfer Manual—Protecting Security Communications," issued 1999 (Ref. 48)

4.1.4 Security Response/Neutralization—10 CFR 73.100(b)(4)(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 should 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: Licensees should complete a defense-in-depth analysis to identify the effects of vehicle-borne explosives on the response element of the physical protection program. This analysis can credit vehicle control measures, fighting position design, personal protective equipment, and other programmatic aspects of the physical protection program.

  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 1.5 times the 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. Applicants and licensees should refer to Revision 1 to RG 5.69 for additional guidance regarding the range of the potential hand-carried and vehicle borne explosives,

charge weights, and relative effectiveness factors against which physical protection programs and protective strategies must be designed to defend.

B. Offsite response—The response force, including law enforcement or other offsite armed responders, should 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
- documenting in its physical security plan (PSP) and safeguards contingency plan (SCP) the security licensing basis for how law enforcement or other offsite armed responders will be relied on to perform interdiction and neutralization functions.
- describing in the PSP and SCP how law enforcement or other offsite armed responders will provide the necessary responses to implement contingency responses to achieve the performance objectives and meet the requirements of 10 CFR 73.100(b).
- capturing specific law enforcement or other offsite armed responders' capabilities, including but not limited to, the minimum number and positions (i.e., patrol officer, tactical team member) of available responding armed responders, response equipment, tactical capabilities, and response times, and the relevant plant structures and systems required for providing delay.
    - When the licensee relies on law enforcement or other offsite armed responders to perform the interdiction and neutralization function, the licensee should ensure that the activities, tactical response drills and force-on-force exercises are planned and conducted in a manner to make them available to the LE other offsite armed responders. The licensee should conduct a sufficient number of security drills and exercises to enable law enforcement or other offsite armed responders who may implement contingency response and licensee protective strategy to participate in the licensee-conducted drills and exercises.
- establishing standards for adequate security of the offsite facilities that house armed responders and these standards should be included in its arrangement for proprietary and contract offsite security responders. If the licensee leases offsite facilities, the lease should include standards for the adequate protection of these facilities including protection against unauthorized access by personnel or vehicles, disruption of communications, delay or blockage of the facilities' egress routes.

If a PSP relies on law enforcement or other offsite armed responders for interdiction and neutralization functions, the licensee should develop a written law enforcement response plan (i.e. memoranda of understanding (MOUs)) that documents coordination between the licensee and law enforcement or other offsite armed responders expected to respond to the site during a contingency event.

The MOU agreement should establish the mutually agreed upon commitments and acceptance of performing interdiction and neutralization functions to defend the licensed facility.

To maximize the likelihood that the required offsite assistance will be available and reliable at all times, a licensee should consider establishing MOUs with at least two offsite armed response organizations that have not entered into a mutual aid agreement with each other and that are independently capable of interdicting and neutralizing the DBT. The safeguards details of how an organization will respond to contingency events should be described in the license's SCP.

The MOU should include both the licensee and offsite armed response organization's activities to plan, train, drill, and exercise contingency response to ensure they can respond to interdict and neutralize the DBT at all times, including:

- specific commitments of resources (people and equipment) that will be available and the minimum response times needed to respond and successfully interdict and neutralize the DBT adversary.

- mutually agreed upon frequencies to support licensee drills and exercises. Licensees must meet the frequency of tactical response drills and force-on-force exercise requirements.

- response contingencies that may affect the availability of an offsite armed response organization to respond, such as budgetary constraints, events that would likely compete for resources, or ongoing responses other than to a licensee plant.

- plant familiarization and walkdown frequencies – once a year, or more frequently for responders who are unable to identify and self-navigate to all areas of the facility associated with their security contingency plan or protective strategy implementation duties and responsibilities.

- reliability of communications by testing communications – twice daily, morning and afternoon.

- 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 and RG 5.54.

The following activities should be considered for law enforcement or other offsite armed responders:

- Familiarize and walkdown site and facility, structures and systems, plant hazards, and operations

    - Maps or sketches depicting the owner controlled and protected areas,

    - General arrangement or plant equipment drawings for all elevations in the industrial portions of the facility,

- Pre-fire plans or similar drawings for all other buildings in the protected area and potential safety-related buildings in the owner controlled area,
- Door- and barrier-related information, and
- Communications and photographic information.

- Plan specific security tactical missions
- Test communication systems
- Conduct tabletop exercises
- Perform limited and field tactical response exercises
- Capture, track, and disposition lessons learned from drills and exercises.
- Document and describe, in the SCP, how law enforcement or other offsite armed responders will implement the licensee's physical protection program to defend against threats to its facility, up to and including the DBT of radiological sabotage in order to meet the requirements of 10 CFR 73.100(b)(4)(iv)(A)(*4*).
  - The SCP should describe in sufficient detail how law enforcement or other offsite armed responders will fulfill interdiction and neutralization of threats up to and including the DBT of radiological sabotage, in lieu of onsite licensee personnel. The SCP should:
    - organize the response effort using law enforcement or other offsite armed responders,
    - provide predetermined, structured response by law enforcement or other offsite armed responders and licensees to safeguards contingencies,
    - ensure the integration of response by all entities responding, and
    - achieve a measurable performance in response capability.
  - The SCP should describe the planning and organizing of the enforcement or other offsite armed responders and the licensee's resources in such a way that the law enforcement or other offsite armed responders (i.e., participants) will be identified, their responsibilities specified, and the responses coordinated. The SCP should also describe what constitutes a timely response, indicate offsite responders and licensee contingency response personnel training and qualification, and detail how coordination between law enforcement, other offsite armed responders, and licensee contingency response personnel will be accomplished.
  - The licensee should provide descriptions in the SCP in sufficient detail to address how plant systems and components and facility configurations are designed to provide security delay functions and integrated with the law enforcement

contingency response plan (LECR). These systems, components and facility configuration must ensure that law enforcement or other offsite armed responders have sufficient time to respond to a site and conduct the tactical operations required to interrupt the DBT adversary tasks before the adversary can defeat or circumvent the licensee's established delay systems.

- In order to meet the requirements of 10 CFR 73.100(b)(4)(iv)(A)(*4*), the SCP should include descriptions of the activities described in the licensee's MOU with the law enforcement or other offsite armed response's LECR. The LECR should be maintained independent of the licensee security plan (i.e., physical protection, training and qualification, safeguards contingency, and cybersecurity) to establish process and procedures necessary to maintain and implement the contingency response and assure integration of necessary licensee personnel and LE for detection, assessment, and interdiction and neutralization functions of the physical protection program designed to prevent the DBT of radiological sabotage from causing a significant release of radionuclides from any source that would endanger the public.

- The licensee should describe management measures and controls in the SCP to include the management and control of changes to the MOU with any law enforcement or other offsite armed responders that is relied upon to fulfill the interdiction and neutralization functions.

- The licensee should establish measures and controls to assure the identification, tracking, and disposition of corrective actions and lessons learned associated with the performance of law enforcement or other offsite armed responders related activities.

- A licensee should maintain records in the possession of the licensee for a period of no less than 3 years.

Appendix D has additional details regarding the type of reactor facility information licensees should provide to LE or other offsite armed responders. It contains sensitive information and is not publicly available.

Additional considerations when relying on a combination of onsite armed responders and law enforcement or other offsite armed responders:

- Licensees should describe relevant information in their PSP and SCP and incorporate necessary elements into their security training and qualification programs.

- When a licensee relies on a combination of onsite armed responders and law enforcement or other offsite armed responders to interdict and neutralize threats up to and including the DBT, the licensee should coordinate, plan, and operate with those law enforcement or other offsite armed responders in a manner that is consistent with the National Incident Management System (NIMS) or other similar framework that the law enforcement or other offsite armed responders may use. Adhering to NIMS concepts, principles, and methodologies to the extent practical should minimize the amount of new information that the law enforcement or other offsite armed responders will need to learn and enable those responders to focus on elements that are important or unique to a licensee's facility.

- Licensees should identify in their SCPs all key locations necessary to facilitate an effective response by law enforcement or other offsite armed responders. Examples of key locations

for law enforcement or other offsite armed responders may include optimal in-plant locations for placing portable radio frequency repeaters (if necessary); police stations or substations; dispatch centers; near-site assembly, staging, or rehearsal areas; incident command posts; and tactical operations centers. Key locations for licensee proprietary or contracted offsite armed responders should include the facilities that house those responders.

- Licensees should identify and document the primary, secondary, and when necessary, tertiary travel routes from offsite armed responder key locations or facilities to pre-identified staging areas (if applicable) and protected area entry points. This information should help licensees determine the extent to which compensatory measures may be necessary to address potential degradations or compromises that could be caused by threats up to and including the DBT, or by route disruptions associated with proximate, non-hostile incidents (e.g., parades, protests, natural disasters, vehicle accidents, etc.).

- Licensees should ensure that law enforcement and other offsite armed responders have appropriate dosimetry, including emergency electronic dosimetry. Emergency electronic dosimeters help to minimize law enforcement or other offsite armed responders' exposure to radiation by providing real-time indications of accrued dose and alarming if the responders enter areas with radiation dose rates above the devices' programmed set points.

- Licensees should establish, implement, maintain, and document communications that are necessary to facilitate an effective response by LE or other offsite armed responders, including the use of special signals. Examples include, but are not limited to:

    - Sign and countersign

        - A sign and countersign is a set of pre-identified codes, signals, or other measures that law enforcement responders and a licensee's onsite and other offsite armed responders can use to establish whether a person(s) they encounter is authorized to be in an observed location. When a responder presents a sign (i.e., verbally or non-verbally challenges someone), the person(s) being challenged should respond by saying or displaying the approved countersign. Should the person(s) being challenged fail to present the appropriate countersign, responders should consider the person(s) being challenged to not have authority to be in the observed area.

        - Signs and countersigns should be developed and disseminated by a central authority, such as the management for a licensee's security organization. If a licensee decides to use signs and countersigns it should be appropriately protected. The licensee should also establish, implement, and maintain a secure method for providing signs and countersigns to LE or other offsite armed responders before their effective periods begin.

        - An example of a simple sign/countersign is the Odd Number System. A responsible authority (e.g., management for a licensee's security organization) pre-identifies a different odd number for each day. The challenge number can be any number less than the pre-identified odd number-of-the-day. The response should be the number that must be added to challenge number to equal the pre-identified odd number-of-the-day. For example, if the number-of-the-day is 7 and the challenge is 3, the response should be 4.

- Running password

    - A running password can be useful when law enforcement or other offsite armed responders need to approach known onsite armed responders or armed response positions under exigent circumstances, such as when the law enforcement or other offsite armed responders are redeploying while being engaged by an adversary. A running password is typically used in conjunction with the number of friendly personnel who will be authorized to pass the armed responder or armed response position. For example, if the running password is "Responder" and there are three law enforcement responders running toward one of a licensee's known armed response positions, the law enforcement responder first approaching the position would declare, "Responder three," using the most appropriate communications method (e.g., yelling, radio, etc.). The armed responder in the known position would allow the first three approaching individuals to pass before resuming normal challenging or engagement protocols.

    - The armed responder in the known position should verify the identity of the personnel who use a running password (or arrange for another security member to perform the verification) as soon as it's safe to do so (e.g., no immediate threat to the known position or those who used the running password). The armed responder in the known position should also notify the security command and control element when a running password has been used, so security leadership can consider implementing a different running password. An adversary may hear someone using a running password and use the same password to attempt to deceive the same or another armed responder.

    - Running passwords should be developed and disseminated by a responsible central authority, such as the management for a licensee's security organization. If a licensee decides to use running passwords. The licensee should also establish, implement, and maintain a secure method for providing running passwords to law enforcement or other offsite armed responders before their effective periods begin.

- Color of the day

    - Licensees may want to consider establishing a color of the day and an appropriate method for displaying it. Unlike signs, countersigns, and running passwords, a color of the day is a passive measure that can reduce the time it takes for armed responders to identify other armed response personnel. Before establishing and implementing a color-of-the-day measure, a licensee should consider whether the color and its display method (e.g., armband, Velcro patch, etc.) will enable rapid visual discrimination from the distance(s) the licensee's protective strategy may require, any potential visibility limitations that may be present, and the degree to which, if any, the color or its display location may aid an adversary's ability to identify and aim at responders.

- Colors of the day and any approved display method(s) should be developed and disseminated by a central authority, such as the management for a licensee's security organization. If a licensee decides to use colors of the day, it should develop and control them appropriately. The licensee should also establish, implement, and maintain a secure method for providing colors of the day, any approved display method(s), and the process for implementing the measure to law enforcement or other offsite armed responders before their effective periods begin.

- Licensees utilizing colors of the day should train its onsite and offsite armed responders to recognize when someone inappropriately uses a color of the day. For example, a person may attempt to gain access to a protected area or other limited-access area using the color of the day when a licensee's security organization did not initiate that measure during a safeguards contingency response. Such occurrences could indicate the presence of an active insider, either the person inappropriately using the color of the day or someone who may have provided that person with the knowledge or material.

- Infrared or thermal devices

  - Infrared chemical sticks (e.g., ChemLights©) and markers (e.g., LightShapes©) are passive devices that use chemical substances to produce infrared light.

  - Infrared patches are passive devices that use infrared film to produce an infrared glow. The infrared glow pattern is determined by the design of the patch. Licensees considering this device should use covert patches, when possible. Covert patches will not reflect light in the visible spectrum.

  - Thermal patches and markers are passive devices that use a thermal film to reflect heat and provide a clear contrast between the patch and the surrounding environment. Thermal markers are commonly used on the roofs of emergency response vehicles so incident command and control staff can see precise response vehicle locations when using aerial surveillance assets (e.g., drones, helicopters, fixed-wing aircraft). Licensees should consider whether it would be appropriate to use thermal markers to identify facility locations, such as structure entrances, response positions, or areas associated with mitigation activities.

  - Active infrared and thermal beacons are devices that emit multispectral and omnidirectional infrared light. Infrared and thermal beacons can be designed to emit both visible and infrared light, or only infrared light. Models that emit only infrared light are considered to be more suitable for IFF during safeguards contingency events. Infrared or thermal beacons that also emit visible light are typically used for search and rescue or other operations that are conducted in permissive (i.e., non-hostile) environments.

  - Licensees that have access to infrared tactical aiming lasers or portable infrared light sources should consider establishing and implementing visual sign(s), countersign(s), and other information transfer protocols that its onsite

and offsite armed responders, and LE, can use in conjunction with those devices. Infrared lasers and portable infrared lights can enable personnel to identify each other and potentially communicate additional information (e.g., a hazard or other area of interest) without disclosing their positions to those without appropriate equipment, as could be the case when using visible light.

C. Remotely Operated Weapons Systems (ROWS)—Where engineered remotely controlled weapon systems are relied on for interdiction and 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. Licensees should ensure that their ROWS designs do not contain any single-point failures that can be exploited by an active insider, such as those associated with the lethal force authorization and duress functions.

    - A ROWS design should have at least two separate locations from which deadly force authorization can be implemented and at least two separate people on shift and assigned to different locations who can authorize ROWS operators to use deadly force. Deadly force should be able to be authorized by any one of the individuals with that authority at any of the locations where deadly force can be authorized. The ROWS design should not allow a single person to simply not act when expected (e.g., refuse to authorize deadly force, hide or dispose of a key) or commit an unintentional error that results in a licensee relying on ROWS being unable to maintain the capability to interdict and neutralize threats up to and including the DBT.

    - ROWS should be designed to require at least two duress signals from independent and separate locations before any weapons platform, control console, or other ROWS component is disabled in response to a duress function. The ROWS design should not allow a single person to disable one or more ROWS weapons platforms, control consoles, or other components. An active insider could intentionally exploit a ROWS design that responds to single duress signals, and someone who erroneously activates the duress function could unintentionally disable one or more ROWS components, which could interfere with, or prevent, a licensee from effectively interdicting and neutralizing threats.

- Licensees should consider that the number of ROWS weapons platforms that can be active at any time is typically limited to the number of control consoles. Some ROWS designs permit a control console to operate any weapons platform, but a control console can typically operate only one weapons platform at a time. This limitation is important to recognize because it

could determine whether a licensee will have intersecting fields of fire for each of the DBT's maximum number of potential protected area entry points, and for other interdiction and neutralization points at other layers of a licensee's protective strategy.

- A ROWS design should have enough ROWS weapons platforms at each interdiction and neutralization layer of a licensee's protective strategy to ensure that the loss of any one weapons platform will not adversely affect the licensee's ability to defend against threats up to and including the DBT.

- Reliable primary and backup power (e.g., an uninterruptible power supply) are provided for continuity of system functions until the adversary interference precluded time.

- 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.

D. Compensatory measures for a degradation or absence of law enforcement or other offsite armed responders—The licensee should develop criteria and compensatory measures for the degradation or absences of LE or other offsite armed responders to fulfill the interdiction and neutralization functions in accordance with 10 CFR 73.100(b)(4)(iv)(A)(*5*). In addition, compensatory measures must provide a level of protection that is equivalent to the protection that was provided prior to the degradation or inoperability of the security structures, systems, or components in accordance with 10 CFR 73.100(h)(3). One option is for the licensee to coordinate, plan, and train with at least two independent LE or other offsite armed response organizations who have sufficient capabilities to interdict and neutralize threats up to and including the DBT within the time provided by the licensee facility's security delay features. Preparing for a security contingency event in this manner, a licensee should be able to orchestrate support more easily from the secondary LE or other offsite armed response organization when the licensee becomes aware that the support needed from the primary offsite response is degraded or unavailable.

In accordance with 10 CFR 73.100(b)(4)(iv)(A)(*5*) the licensee must identify suitable compensatory measures that meet the requirements of paragraph 10 CFR 73.100(h)(3) to address the degradation or absence of LE or other offsite armed response organizations. The licensee should assess possible situations that could result in the unavailability of its LE or other offsite armed responders. The licensee's compensatory measures should be described in the PSP and should identify the timeframe(s) for implementation of those measures to ensure that the licensee continues to maintain, at all times, the capability to interdict and neutralize threats up to and including the DBT.

In accordance with 10 CFR 73.100(b)(4)(iv)(A)(*5*) the licensee should establish criteria for when to implement the compensatory measures that address the possible situations where the LE or other offsite armed responders may be unavailable or only capable of providing a limited response. The implementation time(s) must enable the licensee to continue to satisfy the DBT interdiction and neutralization functions required by 10 CFR 73.100(b)(4)(iv) and 10 CFR 73.100(b)(4)(iv)(A)(*5*).

To ensure that equivalent protection is provided by compensatory measures, the licensee should evaluate the appropriate compensatory measures they would employ. The evaluation should:

- identify how the degradation affects the ability of LE or offsite armed responders to fulfill the interdiction and neutralization functions to protect the plant against threats up to and including the DBT of radiological sabotage, with the most security significance attributed to the degradation or loss of capability to interdict and neutralize the DBT adversary.

- consider how the degraded situations affect interdiction and neutralization functions to determine the equivalent compensatory measure that the licensee must implement. One acceptable approach could be to provide response by the licensee's available assets and staffing necessary to provide equivalent capability to compensate for the degradation. Use of other LE or other offsite armed responders could also provide an acceptable approach.

- establish procedures for evaluating the measures should take into consideration the safety/security interface, including the requirements of 10 CFR 73.58 that pertain to plant configurations and facility conditions, and the interfaces that would exist during a security response.

- focus on specific degradations and the implementation of compensatory measures that would provide equivalent functions, to include consideration of changes in plant safety operations, conditions, and/or configurations that may compensate for the degradation (e.g., safe shutdown, reduce radiological hazards, change material configurations, additional barriers, increase delay, etc.).

- develop a reference of pre-determined actions or measures applicable to their site, which identifies potential degradations and pre-determined measures to compensate for the degradations.

- account for additional staffing at a certain time or during certain situations. The licensee should consider this additional staffing during workforce planning so that it does not create vulnerabilities or degradation in the required capabilities to perform interdiction and neutralization functions.

The degradation that should be considered in the evaluation may range from individual degradation to multiple degradation or complete loss of interdiction and neutralization functions (i.e., absence of LE or other offsite armed responders).

- During this evaluation, the staffing or assets to compensate for multiple degradations should be considered.

- Then, the overall interdiction and neutralization functions should be reviewed to determine the impact of applied compensatory measures with respect to compensating the LE or other offsite armed responder capability to perform security operations and execute the required actions to interdict and neutralize threats up to and include the DBT adversary.

The licensee should be aware that, as a general policy, armed security personnel serving as a compensatory measure for functions other than interdiction and neutralization functions should not be considered simultaneously available for the compensatory measure intended to compensate

for security response to implement interdiction and neutralization. For example, a licensee's capabilities to assess, detect, delay, interdict and neutralize should be maintained through the implementation of compensatory measures.

In determining the proper application of appropriate compensatory measures in a situation of degradation of LE or other offsite armed response organizations, the licensee should consider the use and application of all security assets with the minimum standard complement of security staffing. This approach would provide continued assurance that the integrity of the licensee's physical protection program will be maintained by verifying that the measures the licensee employs to compensate for degradation in a situation do not reduce the site's overall physical protection capabilities.

Immediate measures provide a reduced level of protection to a degradation or loss of functions to minimize the possible exploitation until appropriate compensatory measures can be implemented. Immediate measures represent the best protection a licensee can provide with onsite resources during an unanticipated or unforeseen degradation or failure of a security SSC or function. Consistent with 10 CFR 73.100(h)(3), compensatory measures must provide an equivalent level of protection until the degradation or loss of interdiction and neutralization functions is corrected. Licensees should anticipate and thoroughly evaluate potential degradations to security SSCs and offsite armed response and identify appropriate compensatory measures. Licensees should be prepared to implement compensatory measures for reasonably foreseeable degradations or failures, and to the extent practical, not rely on immediate measures.

When degradation consisting of the absence of law enforcement or other offsite armed responders to perform interdiction and neutralization functions is identified or discovered, licensee must, as soon as possible, initiate corrective actions and restore functions in a graded timeframe appropriate and commensurate with the significance of the degradation.

E. 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) should 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.

- Consider the design and operation of the facility and the necessity of operator actions that may be interrupted by an adversary, and plan delay features in accordance with guidance on the crediting of operator actions found in RG 5.81 to support necessary functions.

- 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.

F. Engineered passive or active barrier systems—Consistent with the definition in 10 CFR 73.2 for physical barrier that "any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended," the alternative means for physical barriers should be constructed of material suitable to achieve the security delay and access control.

Examples of engineered active or passive systems that may be used to perform delay functions include, but are not limited to, those described in SAND2007-5591, Security Assessment Technical Manual (e.g., sticky foam, obscurant and deployable barriers, munition-based access denial systems, gabion-filled walls, Silent Defender, Virtual Presence and Extended Defense system, etc.), engineered barrier systems (e.g., gates, vault type doors, turnstiles, etc.) currently deployed at currently operating power reactors, and new technologies (e.g., millimeter wave, long range acoustic device, etc.).

The capability to implement an appropriate security delay should be met and maintained by the design of a physical protection system to achieve the performance criteria where the design of SSCs relied on for delay functions provides assurance of necessary and sufficient time for licensee security responders, LE, or a combination of licensee security responders and LE to interdict and neutralize the DBT before it achieves radiological sabotage.

To provide adequate delay, licensees or applicants should design their security systems to be able to delay the DBT adversary for a time equal to or greater than a site's adversary interference precluded time (AIPT), based on the process described in Appendix C, "Adversary Interference Precluded Time," of this guidance.

- The design of security delay systems should be appropriately layered for defense-in-depth.

- Design of security delay systems may include passive barriers that obstruct or physically delay the passage of person, vehicles, and material.

- Acceptable delay, where appropriately designed, may include physical space that provides delay by means of physical separations, which are evaluated and considered in developing response timelines for security or LE response.

- The alternative means of a physical barrier for security delay may also consider engineered active systems (e.g., remotely operated weapon systems, munition-based access denial systems, counter sniper remotely operated system) that can perform neutralization functions, which could successfully prevent the DBT adversary from performing or completing tasks.

- The design of engineered physical security SSCs that perform neutralization of the DBT adversary should take into consideration their potential impact on security responders and the effectiveness of the security response. Licensees may take credit for the required security delay functions performed by such physical security SSCs if appropriate. For example, the design of engineered physical security SSCs that perform neutralization functions, engineered fighting positions relied upon for protecting engineered systems, and components relied upon to perform neutralization functions should provide overlapping fields of fire. The design configuration should provide layers of opportunities for security response, with each layer assuring that a single failure does not result in the loss of capability to neutralize the DBT adversary.

    - The licensee should design its physical barrier system for automated access control to include anti-piggybacking, anti-tailgating, and anti-pass back functions for control of personnel and material.

    - NUREG-1964, "Access Control Systems: Technical Information," provides physical barrier configurations that may be considered in a licensee's design of protected area personnel access control portals.

    - The licensee should design the configuration of physical barrier systems for access controls to satisfy the requirements of 10 CFR 73.100(b)(4)(vi). The licensee may use the acceptance criteria in Standard Review Plan Sections 13.6.1 and 13.6.2 to assist in the design of access control measures.

    - Physical vehicle barrier system designs are designed and installed to prevent vehicles from entering (or leaving) and may consist of passive (e.g., fences, walls, concrete blocks, concrete and sand barriers, shallow vehicle barriers, etc.) and active (e.g., pop-up vehicle barrier, hydraulic barriers, etc.) systems. Vehicle physical barriers may also use natural terrain (e.g., rocks, mountains, rivers, thick forests, ravines, etc.). The vehicle control measures (e.g., passive and active barrier systems) to deny land or waterborne vehicle bomb assaults should be located at a bounding minimum safe stand-off distance to adequately protect all SSCs required for safety and security from an explosion based on the maximum DBT quantity of explosives.

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

- RG 5.54
- RG 5.76, “Physical Protection Programs at Nuclear Power Reactors,” (SGI) (Ref 11)
- NUREG/CR-0543 SAND2007-5591, “Nuclear Power Plant Security Assessment Technical Manual,” issued 2007 (Ref. 24)
- 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. 49)
- Interagency Remotely Operated Weapon Systems (IROW)-002, “Performance Specification System Specifications for the Interagency Remotely Operated Weapon Systems (IROWS),” dated February 2009 (Ref. 50)
- SAND2013-0038, “Security-by-Design Handbook,” issued 2013 (Ref. 51)
- NUREG/CR-7201, “Characterizing Explosive Effects on Underground Structures,” issued September 2015 (Ref. 20).

4.1.5 Control Measures Protecting against Land and Waterborne Vehicle Bomb Assaults 10 CFR 73.100(b)(4)(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 containing critical reactor safety SSCs (e.g., reactor building) 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 the maximum DBT quantity of explosives, as described in Revision 1 to 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 4.1.4.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. 52), or International Workshop Agreement (IWA) 14-1:2013, "Vehicle Security Barriers—Part 1: Performance Requirement, Vehicle Impact Test Method and Performance Rating" (Ref. 53).

- 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 the maximum DBT quantity of explosives, as described in Revision 1 to 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, "Physical Protection Programs at Nuclear Power Reactors," (SGI) (Ref 11)

- USACE, "Update of NUREG/CR-6190 to Reflect Revised Design Basis Threat," dated March 2004 (Ref. 54)

- USACE PDC-TR-06-05, "Evaluating Adequacy of Landform Obstacles as Vehicle Barriers," dated August 2007 (Ref. 55)

- USACE PDC-TR-06-06, "Passive Inertial Vehicle Barrier Design Guide," dated August 2007 (Ref. 56)

- USACE Protective Design Center Technical Report PDC-TR-06-09, "Vehicle Access Control Point Guidance," issued 2008 (Ref. 31)

- NUREG/CR-7201, "Characterizing Explosive Effects on Underground Structures," issued September 2015 (Ref. 20).

4.1.6 Access Control Portals—10 CFR 73.100(b)(4)(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, "Physical Protection Programs at Nuclear Power Reactors," (SGI) (Ref 11)
- USACE Protective Design Center Technical Report PDC-TR-06-09, "Vehicle Access Control Point Guidance," issued 2008 (Ref. 31)
- SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," issued 2007 (Ref. 24)
- SAND99-2168

4.1.7 Target Sets

Consistent with 10 CFR 73.100(b)(5) and 10 CFR 73.100(b)(6), the licensee must identify and analyze site-specific conditions, including achievable target sets, that may affect the physical protection program needed to implement the requirements of this section. Achievable target sets are used to inform the design of a licensees' protection program in order to prevent a release exceeding the reference values defined in 10 CFR 53.210.

Staff Regulatory Guidance Position 8.8, "Screen for Achievable Target Set Elements," of RG 5.81, allows licensees to determine which target sets are achievable based on three criteria. An achievable target set is:

- within the capabilities of the design basis threat adversary to compromise, destroy, or render non-functional;
- cannot be mitigated after adversary interference is precluded and prior to a release of radionuclides exceeding dose reference values defined in 10 CFR 53.210; and,
- if defeated, result irreversibly in exceedance of the dose reference values defined in 10 CFR 53.210.

4.1.8 Performance Evaluation Program

Consistent with 10 CFR 73.100(b)(7), each licensee must establish, implement, and maintain a performance evaluation program (PEP). Each licensee must 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)(7). RG 5.75 provides additional details regarding the PEP.

Consistent with Staff Regulatory Guidance Position 5, "Performance Evaluation Program," of RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities," the tactical response drills may include tabletop exercises, limited-scope tactical response drills, and timeline verifications that provide a structured process to train response personnel and evaluate key elements of the safeguards contingency response implementing the protective strategy by focusing on specific aspects of the strategy without conducting a fully integrated force-on-force (FOF) exercise.

If law enforcement or other offsite armed responders provides response functions, guidance for the conduct of contingency response and law enforcement or other offsite armed response force-on-force exercises can be found in Appendix A, "Recommended Guidelines for Conduct of Law Enforcement and Other Offsite Armed Response Contingency Response Drills," and Appendix B, "Recommended Guidelines for Conduct of Law Enforcement and Other Offsite Armed Contingency Response Force-On-Force Exercises."

4.1.9 Access Authorization Program

Consistent with 10 CFR 73.100(b)(8), each licensee must establish, implement, and maintain an access authorization program in accordance with 10 CFR 73.56 or 10 CFR 73.120, as applicable, and describe the program in the physical security plan. RG 5.66 contains further guidance on the implementation of the access authorization plan.

4.1.10 Cybersecurity Program

Consistent with 10 CFR 73.100(b)(9), each licensee must 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 RG 5.96.

4.1.11 Insider Mitigation Program

Consistent with 10 CFR 73.100(b)(10), the licensee must establish, implement, and maintain an insider mitigation program and describe the program in the physical security plan. The insider mitigation program must 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 must integrate elements of the access authorization program, fitness-for-duty program, cybersecurity program, and physical protection program. This integration ensures the licensee's capability to identify and mitigate potential insider activities, including, but not limited to, tampering, sabotage, and unauthorized disclosure of sensitive information. No single element of the physical protection program, access authorization

program, cyber security program, or fitness-for-duty program is sufficient by itself to provide the level of protection required. Therefore, the effective integration of these four programs is essential to achieving defense-in-depth against insider threats.

Licensees should not limit physical protection elements of the insider mitigation program to a fixed set of elements. Rather, the insider mitigation program should be adaptive and may need to include physical protection elements that are not specifically prescribed to meet the performance requirements of 10 CFR 73.100(b) to protect against the design basis threat of radiological sabotage, including knowledgeable active or passive inside assistance as described in § 73.1 and RG 5.69. The access authorization- and fitness-for-duty-related measures in licensees' insider mitigation programs do not relieve licensees from having to establish, implement, and maintain security system designs or physical protection-related measures to adequately defend against the active insider threat attributes of the design basis threat of radiological sabotage.

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.

4.1.12 Corrective Action Program

Consistent with 10 CFR 73.100(b)(11), the licensee must 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.

4.1.13 Integration of Site Plans and Procedures

Consistent with 10 CFR 73.100(b)(12), the implementation of security plans and associated procedures must be coordinated with other onsite plans and procedures to preclude conflict during both normal and emergency conditions. To accomplish this, the licensee must identify and resolve areas of potential conflict. Each licensee must consider the requirements of 10 CFR 73.58 during this review. RG 5.74 contains further guidance.

4.2 Security Organization

Consistent with 10 CFR 73.100(c), the licensee must 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 must 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:

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 The licensee should ensure that only persons who have been specifically trained, equipped, and qualified in accordance with the licensee's approved training and qualification plan perform activities that are required for or support the licensee's implementation of the physical protection program.

4.2.6 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.

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

4.3 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 must 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:

4.3.1 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.

4.3.2 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.

4.4 Training and Qualification Program for Licensee Security Personnel

Consistent with 10 CFR 73.100(e), the licensee must 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.

4.4.1 The licensee must 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.

4.4.2 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.

4.4.3 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.

4.4.4 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.

4.4.5 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.

4.4.6 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.

4.4.7 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.

4.4.8 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.

4.4.9 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.

4.4.10 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.

4.5 Security Reviews

4.5.1 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 must be designed to ensure that the physical protection program maintains effectiveness and meets requirements.

4.5.2 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.

4.5.3 Physical protection program reviews must 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.

4.5.4 Consistent with 10 CFR 73.100(f), individuals independent of licensee management and personnel who have direct responsibility for implementing the physical protection program must 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.

4.5.5 Consistent with 10 CFR 73.100(f)(3), reviews of the security program must 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.

4.5.6 Consistent with 10 CFR 73.100(f)(4), a report must 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.

4.5.7 Consistent with 10 CFR 73.100(f)(4), all reports of such reviews must 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).

4.6 Performance Evaluation

Consistent with 10 CFR 73.100(g), licensees must 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 4.1.8 of this document provides guidance to establish, implement, and maintain a PEP. RG 5.75 contains further guidance on an acceptable method to meet this requirement.

4.7 Maintenance, Testing, Calibration, and Corrective Actions

Consistent with 10 CFR 73.100(h), the licensee must 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.

4.7.1 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).

4.7.2 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 law enforcement agencies (LLEAs), to include backup communications equipment, should be tested for operability at least once each day.

4.7.3 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.

4.7.4 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. 57).

4.7.5 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.

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

4.7.7 The licensee must establish and implement timely compensatory measures for degraded or inoperable security SSCs to meet the requirements in 10 CFR 73.100. Compensatory measures must 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.

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

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

4.8 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.

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

4.8.2 The suspension of security measures must be reported and documented in accordance with the provisions of 10 CFR 73.1200 and 10 CFR 73.1205. RG 5.76 contains further guidance.

4.9 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 must maintain all records required to be kept by Commission regulations, orders, or license conditions, until the Commission terminates the license for which the records were developed and must maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission, (3) if a contracted security force is used to implement the onsite physical protection program, the licensee's written agreement with the contractor must be retained by the

licensee as a record for the duration of the contract, and (4) review and audit reports must be available for inspection, for a period of 3 years. RG 5.76 contains further guidance.

5. Security Requirements for the Possession and Loading of Fresh Fuel into a Manufactured Reactor

5.1 Physical Security

10 CFR 53.620(d)(2)(i), states, in part, that for the protection of SNM of low strategic significance, the licensee is required to meet the requirements of 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" with specific additions and exemptions.

10 CFR 53.620(d)(2)(i)(A) states, in part, that a physical security plan describing the physical security program must be maintained for the possession and loading of fresh fuel into a manufactured reactor authorized by a 10 CFR Part 70 license, regardless of fuel type, enrichment, and quantity.

10 CFR 53.620(d)(2)(i)(B) states that *"The physical security program must be designed to prevent unintended and uncontrolled criticality events."*

Consistent with 10 CFR 70.22(g), 70.22(h), and 70.22(k) a licensee must provide a physical security plan as part of the license application. This plan is required in order for the applicant to demonstrate compliance with the specific physical protection requirements of 10 CFR Part 73 and must be submitted with each application for a license to possess or use SNM (or for a license authorizing transport or delivery of SNM), except for a license to possess, use, or transport less than 10 kg of SNM of low strategic significance, in which case a physical security plan is not required.

Regulatory Guide 5.59, "Standard Format and Content for a Licensee Physical Security Plan for the Protection of Special Nuclear Material of Moderate or Low Strategic Significance" (Ref. 58), provides guidance and describes the information required in the physical security plan submitted as part of an application for a license to possess, use, or transport SNM of moderate strategic significance or 10 kg or more of SNM of low strategic significance and recommends a standard format for presenting the information in an orderly arrangement.

5.2 Cybersecurity

10 CFR 53.620(d)(2)(i)(A) states, in part, that *"…a cybersecurity program must be established for the possession and loading of fresh fuel into a manufactured reactor authorized by a 10 CFR part 70 license, regardless of fuel type, enrichment, and quantity."*

10 CFR 53.620(d)(2)(i)(C) states that *"The cybersecurity program must provide reasonable assurance that a cyberattack does not adversely impact the functions performed by digital assets necessary for implementing the physical security requirements of this section, or the radiation monitoring and criticality requirements in this section or in 10 CFR part 70."*

RG 5.96 provides an acceptable method that applicants and licensees may use for establishing, implementing, and maintaining a cybersecurity program at commercial nuclear plants that are licensed under 10 CFR Part 53 subject to the requirements in 10 CFR 73.110. RG 5.96 also provides acceptable guidance for implementing the fuel load requirements in 53.620(d)(2)(i)(C).

5.3 Access Authorization

Consistent with 53.620(d)(2)(i)(D) all holders of a part 70 license that authorizes loading of fresh fuel into a manufactured reactor must perform the screening required in § 73.67(d)(4) to confirm the identity, trustworthiness, and reliability of individuals prior to granting unescorted access to special nuclear material; these determinations must be documented. Additionally, applicants satisfying the criterion in 10 CFR 73.100(a)(1)(i) may also establish, implement, and maintain their access authorization program under 10 CFR 73.120 as part of their physical security plan before initiating the physical removal of any one of the independent mechanisms to prevent criticality required under § 53.620(d)(1) of this chapter for a fueled manufactured reactor (under 10 CFR 53.610, "Construction).

Regulatory Guide (RG) 5.95, "Access Authorization Program for Commercial Nuclear Plants" (Ref. 59), describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use by licensees to establish, maintain, and implement an access authorization program for commercial nuclear plants under the provisions of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 53, "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants."

The following are general performance objectives and requirements for licensees and applicants satisfying the criterion in 10 CFR 73.100(a)(1)(i) and subject to 10 CFR 73.120:

- Each licensee's or applicant's access authorization program under 10 CFR 73.120 must demonstrate that the individuals specified in 10 CFR 73.120(b)(1)(i–iv) and (b)(2) are trustworthy and reliable, so that they do not constitute an unreasonable risk to public health and safety or the common defense and security. The requirements for the access authorization program include:

- Licensees and applicants satisfying the criterion in 10 CFR 73.100(a)(1)(i) must establish, implement, and maintain their access authorization program under 10 CFR 73.120. The proposed language establishes general performance objectives and requirements providing reasonable assurance that the individuals who are specified in paragraph (b) of 10 CFR 73.120 are trustworthy and reliable.

    - background investigation (BI):

        - personal history disclosure,

        - verification of true identity,

        - employment history evaluation,

        - unemployment/military service/education,

        - credit history evaluation,

        - character and reputation evaluation, and

        - Federal Bureau of Investigation (FBI) identification and criminal history records check.

    - behavioral observation (BO),

- self-reporting of legal actions,
- unescorted access (UA),
- termination of UA,
- basis of determination for access,
- review procedures,
- protection of information,
- audits and corrective action, and
- records.

- Licensees and applicants that implement the access authorization requirements of 10 CFR 73.120 and prepare their programs in accordance with this guidance should include the following statement in their physical security plans: "All elements of RG 5.95 have been implemented to satisfy the requirements of 10 CFR 73.120 related to granting UA and maintaining UA."

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, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests" (Ref. 60), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 53, Subpart H, "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 RG 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, RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors," Washington, DC. **(Official Use Only—Security-Related Information, not publicly available)**

14. NRC, RG 5.96, "Establishing Cybersecurity Programs for Commercial Nuclear Plants licensed under 10 CFR part 53," 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. (ADAMS Accession No. ML072620172)

25 International Atomic Energy Agency (IAEA), Nuclear Security Series No. 8-G, "Preventive and Protective Measures Against Insider Threats," Revision 1, Vienna, Austria, 2020.

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

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

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

29. 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.

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

31. U.S. Army Corps of Engineers (USACE) PDC-TR 06-09, "Vehicle Access Control Point Guidance," 2008, Washington, DC. (ADAMS Accession No. ML083290217)

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

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

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

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

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 NIST, FIPS 140-2, "Security Requirements for Cryptographic Modules," Management, May 25, 2001, 100 Bureau Drive, Gaithersburg, MD, https://doi.org/10.6028/NIST.FIPS.140-2.

44 NIST, FIPS 140-3, "Security Requirements for Cryptographic Modules," Management, March 22 2019, 100 Bureau Drive, Gaithersburg, MD, https://doi.org/10.6028/NIST.FIPS.140-3.

45 NIST, NIST Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations," Revision 2, dated December 2018, 100 Bureau Drive, Gaithersburg, MD, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

46 NIST, NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, dated September 2020, 100 Bureau Drive, Gaithersburg, MD, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

47 NIST, NIST Special Publication 800-82, "Guide to Operational Technology (OT) Security," Revision 3, dated September 2023, 100 Bureau Drive, Gaithersburg, MD, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf.

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

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

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

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

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

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

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

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

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

57. USACE PDC-TR-06-03, “Vehicle Barrier Maintenance Guidance,” Washington, DC, February 24, 2007.

58. NRC, RG 5.59, “Standard Format and Content for a Licensee Physical Security Plan for the Protection of Special Nuclear Material of Moderate or Low Strategic Significance,” Washington, DC.

59 NRC, RG 5.95, “Access Authorization Program for Commercial Nuclear Plants,” Washington, DC.

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

APPENDIX A
RECOMMENDED GUIDELINES FOR CONDUCT OF LAW ENFORCEMENT AND OTHER OFFSITE ARMED RESPONSE CONTINGENCY RESPONSE DRILLS

1 OVERVIEW

1.1 Regardless of whether licensees elect to rely on law enforcement or other offsite armed responders to interdict and neutralize the design-basis threat (DBT) adversary, licensees are required to establish, implement, and maintain a performance evaluation program consistent with the requirements of 10 CFR Part 73.100(g). A performance evaluation program is a critical tool that licensees use to demonstrate and assess the effectiveness of their physical protection programs and protective strategies, including the capabilities of armed responders to carry out their assigned duties and responsibilities during safeguards contingency events.

When relying on law enforcement or other offsite armed responders to interdict and neutralize the DBT adversary, licensees should follow the security drill and exercise guidance in the Staff Regulatory Guidance Position 5 of Regulatory Guide (RG) 5.75 "Performance Evaluation Program."

Licensees should also consider the guidance in Appendices A and B when that guidance would be suitable for drilling and exercising with licensee security personnel who are normally positioned off site.

1.2 This guidance describes one recommended method for the planning and execution of both a tabletop exercise (TTX) and limited-scope drill (LSD) addressing the site-specific law enforcement or other offsite armed responders' contingency response at an operating nuclear power reactor.

1.3 Law enforcement contingency response (LECR) plans should ensure that the capabilities to interdict and neutralize the DBT adversary are met, thereby protecting against the DBT of radiological sabotage. The performance objectives typically describe the expected results from effective implementation of the LECR.

1.4 The types of LECR drills may include the following:

1.4.1 TTXs are performed to demonstrate the protective strategy using a mockup of the facility. TTXs allow security force members to demonstrate their understanding of the protective strategy and their individual role in implementing response to contingency events. This type of drill may also be used as an evaluation tool for determining the effectiveness of the licensee protective strategy that relies on law enforcement or other offsite armed responders to contingency events.

1.4.2 Timeline drills are performed to demonstrate the response timelines established for personnel implementing the LECR to interdict and neutralize the DBT adversary. Drills can be used to test either the validity of the timelines established within the LECR or to test the ability of the LECR's tactical operations to be performed within established timelines to interrupt DBT adversary tasks prior to defeat of licensee delay systems.

1.4.3 LSDs are performed to evaluate the ability of offsite responders to effectively implement their protective strategy responsibilities. They are conducted as needed for each individual, group, or shift to validate and test the protective strategy.

1.4.4 Law enforcement or other offsite armed responders LSD provides an opportunity to practice the response to a hostile action directed against the licensee's nuclear power plant. An LSD should be conducted on a recurring periodic basis to ensure the continued capability to effectively implement the LECR. The frequency of LSD recurrence should be agreed upon by the licensee and law enforcement or other offsite armed responders and in accordance with 10 CFR 73.100(g).

1.4.5 The safeguards contingency plan (SCP) should include a description of the LECR and the memorandum of understanding (MOU) with law enforcement or other offsite armed responders. The licensee, in conjunction with the law enforcement or other offsite armed responders, should review the description of these activities at least annually or when plant changes warrant review and update. Significant organizational changes, either at the licensee or within the law enforcement or other offsite armed responders, may warrant additional reviews. Licensees may elect to include this activity as part of their periodic interactions with law enforcement or other offsite armed responders.

1.5 Key attributes of an LSD with law enforcement and other offsite armed response are listed below.

1.5.1 The LSD utilizes as its base document a fully complete, signed, and issued LECR developed through the combined efforts of the licensee and law enforcement (LE) agency or agencies, which may include State and Federal agencies.

1.5.2 The licensee should be prepared to provide information, plant and operations overview with prominent buildings identified, structural drawings including the location of any safety, security, and emergency preparedness significant structures, systems, and components (SSCs) for LE operational planning and contingency responses to interdict and neutralize threats.

1.5.3 The LSD scenario will postulate responses to threats, with the goal of testing the contingency response strategy to ensure that it can successfully protect against threats up to and including the DBT of radiological sabotage.

1.5.4 The tactical responses may be simulated with outer and inner-plant navigational and communication exercises. Full tactical response is not required to be performed in the field. The licensee may consider the addition of elements into their LECR exercise designed to provide a more interactive exercise. See Attachment C, "Exercise Benefits/Challenges/Limitations," for further information regarding the benefits, challenges, and limitations of various exercise formats.

1.6 Licensee operational personnel may be necessary to simulate any safety and security measures and functions (e.g., Main Control Room, Central Alarm Station), and on-shift safety/security actions.

1.7 Licensee's operations personnel should provide information on any plant safety and security priorities (which will lead to specific law enforcement or other offsite armed responders) or support response related to the planning of on-site tactical operations.

1.8 The conduct of an LSD should include actual or simulated activation and operation of an on-site or near-site Tactical Operations Center (TOC). Depending upon LECR protocols, other facilities defined within the licensee's SCP should be activated or have their activation simulated.

1.9 Licensee personnel, local, State and/or Federal LE agencies should demonstrate the ability to coordinate initial response actions including implementation of plant safe shutdown measures, security delay systems, any autonomous interdiction/neutralization systems, including any coping/mitigation actions, and protection services in both a pre-, active, and post-attack environment.

1.10 To ensure opportunities for demonstration of certain LECR defined capabilities, it will be necessary for the scenario to employ an adversary force with at least the attributes and characteristics of the DBT. In addition, LSD constraints may require that certain events, consequences, or response actions be embellished or presented in a time-compressed fashion. LSD participants should be made aware of these stipulations, and of the expectation to assess, and respond to, the events as presented.

1.11 LSD scenarios should be developed with the goal of testing the licensee's contingency response strategy to ensure that it can successfully protect against the DBT adversary force. Further, performance in these exercises should demonstrate the licensee's ability to successfully implement the physical security plan (PSP) and SCP.

1.12 The NRC recognizes the law enforcement or other offsite armed response will be site-specific and the local and state law enforcement agencies and jurisdictions surrounding different nuclear power plants have varying protocols in implementing the National Incident Management Systems (NIMS). NIMS-related facilities beyond those for on-scene incident command directly located at or near the site should not be needed by the licensee as part of an LSD.

2 LECR LIMITED EXERCISE OBJECTIVES

2.1. To ensure the continued viability of the LECR, the NRC recommends that a licensee maintain a set of LSD Objectives for its facility. These objectives should guide the periodic demonstration of response functions described in the licensee's SCP. The set of objectives should include those functions uniquely performed in response to a hostile action targeting the site.

2.2. The primary and overarching objectives of an LSD should:

2.2.1. ensure an understanding of the tactical integration components of the LECR, including a review of the expected process for Identifying Friend or Foe (IFF)[1] and accessing the plant (e.g., owner-controlled area (OCA), protected area (PA), vital areas (VA)).

2.2.2. provide an opportunity for law enforcement or other offsite armed responders' tactical teams to self-navigate within the OCA or PA, particularly to and from the VA, including those inside the Radiological Controlled Area (RCA) inside the power block.

2.2.3. demonstrate the communication systems, components, processes, and procedures anticipated to be used to support LE or other offsite armed responders' tactical operations under actively hostile conditions, including a radiation hazards environment.

2.3 Additionally, Attachment 1, "Recommended Limited-Scope Drill Objectives," of Appendix A, describe generic guidance that a site should use to develop a set of LSD objectives. Each

recommended objective has an associated description or listing of performance attributes; these attributes define successful objective performance and should be used to develop evaluation criteria for each objective.

2.4 The development of objectives and evaluation criteria should be informed by the site-specific LECR as well as applicable law enforcement agencies (local, state, and federal) and licensee support personnel implementing a potential contingency response. The planning for subsequent LSD performance should include a review of past performance objectives and outcomes.

2.5 The licensee, with law enforcement or other offsite armed responders, should critique TTX and LSD performance to identify opportunities for improvement and as appropriate specific lessons learned should be captured in the licensee's' corrective action program or with other appropriate methods identified by participating LE agencies.

3 LECR LIMITED EXERCISE PREPARATION

This section highlights preparation tasks and support needs unique to an LSD. Each item should be reviewed, and identified actions incorporated into the appropriate LSD preparation, process, and schedule.

3.1 General

3.1.1 An Exercise Manager should clearly communicate expectations to the scenario developers and controllers concerning the handling and forwarding of materials used to prepare for and conduct the LSD. More specifically, personnel must observe all Safeguards Information (SGI) and 10 CFR 2.390, "Public inspections, exemptions, requests for withholding," requirements. The Exercise Manager should identify the site resources necessary to conduct the LSD and ensure that they are scheduled and reserved. Consider items such as the licensee's safety and security personnel and equipment, offsite response personnel and equipment, etc.

3.1.2 Based upon the anticipated level of personnel and their equipment participating in the LSD response, the licensee may notify local news media companies that the site will be conducting an LSD. These contacts are intended to preclude unexpected, and possibly inaccurate or alarming, coverage. This section highlights preparation tasks and support needs unique to an LSD. Each item should be reviewed, and identified actions incorporated into the appropriate LSD preparation, process, and schedule.

3.2 Exercise Support from Security

Licensee safety and security are critical to the successful development and execution of the LSD. Safety and security personnel provide valuable directions and assistance to exercise participants in the following areas.

- Verifying protection of Safeguards Information in LSD materials or during the drill.
- Assuring knowledge of safety and security-related procedures, equipment, and timelines.
- Developing credible DBT attack sequences, and related reports and indications.

- Devising methods to simulate response actions and communications with safety and security facilities and licensee personnel.

- Facilitating LSD planning and preparation with law enforcement (local, State, and Federal) personnel.

- Providing knowledgeable controllers for safety and security facilities/functions.

- Verifying no plant safety operational impact from LSD performance.

- Establishing credible operational objective for LSD contingency response planning.

- Validating site familiarity.

3.3 Tactical Operations Center

3.3.1 Within the Incident Command System (ICS), the Incident Commander (IC) assigns responsibility for establishing a TOC for implementing security operations.

- The TOC IC is responsible for command and control of contingency response to interdict and neutralize the DBT.

- A primary and alternate TOC location should be identified within the SCP and the LECR.

- The selected locations should have the resources and capabilities needed to facilitate performance of TOC functions either in place or readily available as defined within the licensee's SCP.

3.3.2 The LSD TOC should be established in a location that would actually be used during a real event, and not one selected primarily to facilitate LSD performance. LSD focused TOC placement may mask challenges to logistics, communications, and security or preclude the need for important discussions (e.g., how to respond when the TOC is located within an area that must be evacuated).

3.4 Communications

3.4.1 Equipment, resources, and protocols should be in place to facilitate communications among responders at the TOC, security facilities (including licensee alarm station, main control room, and simulated facility locations), tactical teams, and in-fields/on-scene locations.

- These communications paths should be clearly defined and verified (i.e., test communication compatibilities and capabilities prior to the drill).

- The conduct of communications systems testing prior to the drill is preferred, so that the exercise can be conducted within the limitations expected in an actual response condition.

3.4.2 Additional considerations regarding communications are listed below.

- If a communications capability is dependent upon site personnel and offsite armed responders trading radios with one another, ensure that this action can be performed given the security situation created by the scenario.

- If available, evaluate deployment and use of designated offsite response communications vehicles (e.g., a mobile command post) to provide and validate communications interoperability and to provide training to responders.

- Confirm testing alternate means of communication (e.g., by simulating a loss of cellular phone service) at some point.

3.5 Pre-Exercise Briefings and Learning Opportunities

The licensee should provide key exercise participants with a thorough briefing on the proposed scenario, to include the scope, extent-of-play, and performance expectations.

3.6 LECR TTX

3.6.1 The licensee should perform a TTX with the participating law enforcement or other offsite armed responders identified in the LECR prior to the initial LSD and on a periodic basis not longer than every three years.

- A TTX provides law enforcement or other offsite armed responders with an opportunity to review and discuss their respective roles, priorities, and response actions as described in the licensee's SCP and in the LECR.

- Refer to Section 5.0, "LECR Tabletop Exercise Implementation," and Attachment 2, "Recommended Guidelines for Tabletop Exercises," of Appendix A for information on conducting an LECR TTX.

4 SCENARIO DEVELOPMENT

This section highlights preparation tasks and support needs unique to development of DBT level hostile attack scenarios.

Each item should be reviewed, and identified actions incorporated into the appropriate scenario preparation process and schedule.

Scenarios should be developed with the goal of testing the licensee's contingency response strategy, including law enforcement or other offsite armed responders activities relied upon by the licensee to perform interdiction and neutralization of the DBT adversary

4.1 Scenario Team

4.1.1 A team of representatives of the licensee, law enforcement or other offsite armed responders, and other applicable agencies should be used. This should include decision-makers of the local, State, and Federal responds agencies. The licensee should engage law enforcement or other offsite armed responders' personnel early in the scenario

development process to define and discuss scenarios, events, and challenges and to confirm participation in the upcoming exercise.

4.1.2 Drills and exercise scenario materials have the potential to contain safeguards information (SGI). Due to their potential information value, scenario materials should be reviewed and designated as SGI when appropriate. Licensees should share experiences and insights with law enforcement or other offsite armed responders; however, caution should be used to ensure that SGI is protected and not released to unauthorized personnel.

4.1.3 The licensee should take steps to prevent information, such as details of delay features and systems, complete "target set" descriptions, or other plant design and features that would reveal information for DBT sabotage, from being specified in the scenario. If defeat or delay systems and security features and the destruction of a complete target set is necessary to describe exercise objectives, then the scenario should specify other damaged or out-of-service equipment such that the descriptions do not reveal safeguards information. Failure to observe these precautions could result in the release of sensitive information to unauthorized personnel.

4.2 Scenario Development and Key Attributes

4.2.1 When developing a scenario, the first decision to be made is whether the attack will consist of a standalone insider, cyberattack, a standalone vehicle borne explosive, a land-based or waterborne coordinated attack or an attack consisting of a combination of these elements. The scenario team must also determine which primary and, if appropriate, alternate facilities and/or staging areas will be used, as this will likely affect the actual or assumed exercise date and time.

4.2.2 Figure 4-1, *Framework for an Offsite Law Enforcement Agency Contingency Response Limited Exercise*, presents recommended frameworks for developing an LSD scenario. The scenario should consist of two phases, with proposed attributes for each phase. The timeframes for certain actions may be compressed relative to what would be experienced during an actual hostile action. This compression may be necessary in order to conduct the exercise within a reasonable period.

4.2.3 Licensees should ensure that the scenario reflects realistic timelines and notification procedures.

- With respect to the attacking force, the scenario may only specify a number of attackers and associated weaponry in accordance with that defined by the DBT of radiological sabotage.

- The scenario is expected to address the outcomes resulting from a hostile action executed by a force representative of the current DBT.

- To be an effective test of the licensee's contingency response strategy, the scenario events should be designed to challenge the capabilities of the armed responders and be expected to cause, or threaten to cause, damage to irradiated fuel and other sources that could result in significant radiological release.

- The damage, or threat of damage, may be directed towards irradiated fuel in the reactor core, radiological material inventory in systems interconnected to the reactor, or the spent fuel pool.

4.2.4 The scenario events must create a "sense of urgency" in the assessment of plant conditions, response strategies, and dispatch of teams to perform three primary mission types below:

- Locate, interdict, and neutralize the DBT adversary,
- Retake and defend the plant from the DBT adversary, and
- Either (1) or (2) with the additional responsibility of licensee response.

4.2.5 The scenario should present conditions which could, absent mitigating actions, lead to a radiological release. The scenario may be structured such that a radiological release is prevented if exercise players take appropriate and timely mitigating actions.

4.2.6 A LECR exercise scenario should address the following elements:

- Scenario messages containing detail sufficient to ensure that LE responders (e.g., incident command and control, tactical operations, facilities, etc.) fully understand the nature and consequences of the attack.
- During or immediately following a hostile action, the scenario may allow for demonstration of the ability to dispatch licensee personnel to perform time-sensitive actions. The dispatching of licensee personnel in this environment should be coordinated with the LE agency and the IC.
- The scenario should not postulate a condition which enables unchallenged or uncontrolled movement of on-site or law enforcement or other offsite response personnel. Rather, the scenario should cause the IC to assess the active- or post-attack conditions and security/safety in a deliberate and prioritized manner. Example strategies supporting response include use of designated routes and tactical response.
- Ensure that the events and cues necessary to drive decision-making concerning the site-specific contingency responses are well integrated into the scenario timeline and related materials. The number and location of required actions described in the scenario should be commensurate with the nature of the postulated attack.

4.2.7 Options for scenario developers may include the following:

- The exercise's initial conditions may specify that certain equipment is out-of-service (e.g., undergoing maintenance). These out-of-service components may compound the results of the adversary attack. This approach may also assist with the masking of a complete target set, e.g., a critical component is out-of-service, not affected by the attack, and later returned to service to mitigate the event.

- An “insider” may be used to facilitate an attack or exacerbate its effects. Scenarios using an “insider” should include the additional information necessary to play the insider role (e.g., the individual’s name, badge number, location and areas traversed).

- Use of diversionary actions, threats, or attacks at offsite locations.

- Consider response capabilities that support responding tactical teams. Examples include bomb squads, canine units, and aerial delivery assets.

4.3 Scenario Time Progression

4.3.1 The scenario framework may “accelerate” through the initial attack phase to a point where deployment of licensee and offsite agency response assets and implementation of the LECR are assured.

- Exercise messages, or instructions from a controller, should be used to inform participants of the actions which were completed during this time-compressed period (e.g., description of observed initial assault force, suspected hostile locations, mitigative actions attempted, etc.).

- This will allow the IC, in conjunction with key security and operations decision-makers, to demonstrate the ability to plan for, and direct, the deployment of offsite response assets.

4.3.2 Notwithstanding the time compression discussed above, the exercise should be run in real time or as near real time as feasible. More specifically, time jumps should be avoided as these can be a source of confusion to exercise participants. Applicable Federal, State, and local response organizations should be made fully aware of any potential adverse impacts that a time jump or time compression may have on offsite decisions and actions.

4.4 Mini-Scenarios / Master Scenario Events List Detail Descriptions

4.4.1 The following information is typically placed in a stand-alone “mini-scenario” or included in the Master Scenario Events List (MSEL).

4.4.2 To support implementation of DBT adversary task (e.g., coordinated land-based or waterborne) attack timeline, scenario developers should create a detailed description of adversary force movements and actions and related events occurring during the initial attack phase.

- This timeline may include intrusion detection alarms, camera observations, security system actuations, and other information that can be provided by a controller to describe the progress of the attack (e.g., number and location of observed casualties and fires, etc.).

- The DBT adversary attack timeline should not use actual attack progression timing as described in security program documents; however, the selected event sequence and times should be credible.

4.5 Exercise Scenario Confidentiality

4.5.1 The planning, scheduling, and logistical arrangements necessary to conduct a LECR exercise will challenge the normal expectations for scenario confidentiality.

- For example, a TTX will be conducted prior to an LSD.
- In addition, prior reviews and approvals by various licensee and LE personnel may be needed to pre-stage and pre-clear LE responders and vehicles normally associated with contingency responses.

4.5.2 Players should not know any details of the scenario (i.e., specific event timeline and related information).

- The scenario used for an LD should be sufficiently different from that used in the immediately preceding TTX and/or LSD.
- Specifically, the elements and consequences of the hostile action (attack) should be varied between the scenarios, e.g., attack type or direction, number of attackers, attack timeline, damage and casualties, offsite consequences, etc.

4.5.3 Provided that the above confidentiality of scenario planning is met, the same "players" may participate in both a TTX and/or LSD, and the subsequent exercise.

FIGURE 4-1
Framework for an Offsite Law Enforcement Agency Contingency Response Limited Exercise

Initial Response Phase	Continued Response Phase
• Discuss the attack and review immediate response needs • On-site protective measures – "hunker down" – remain in effect • Control Room may request immediate support for limited movement of personnel to support plant stabilization • IC advised of immediate Control Room needs and directs appropriate support (e.g., armed escorts) • law enforcement or other offsite armed responders continue staging; await response direction from IC • IC undertakes discussion and decision-making necessary to support deployment of offsite response assets	• Licensee personnel may move in accordance with directions from IC and Security. Dependent on plant conditions this movement may require offsite response escort • Site liaison personnel report to the TOC • IC develops situation report • Responding tactical teams utilize the site-specific SCP and any additional response tools if developed and available for use • Responding tactical teams should consider simulating some mission planning without the aid of the response tools • Additional mutual aid law enforcement or other offsite armed responders should be dispatched to perform event mitigation actions prior to exercise termination • Communications established between IC, Site, TOC, and Teams, including Team to Team

5 LECR LIMITED EXERCISE IMPLEMENTATION

5.1 This section describes the actions necessary to implement a successful LSD; these actions may be applicable to players or controllers. Included are items the NRC has identified from a review of industry operating experience and observed good practices. Exercise managers should carefully consider each item and incorporate applicable recommendations into the exercise and related implementation processes.

5.1.1 An LSD should demonstrate a coordinated response by law enforcement or other offsite armed responders.

- To effectively demonstrate this objective, a simulated alarm stations can be established (i.e., a control cell) for initiating law enforcement or other offsite armed response.
- Licensee personnel familiar with the operation of these facilities, and capable of simulating their responses, should be assigned as exercise participants.
- Likewise, a knowledgeable individual should be designated to simulate the licensee's operations response.

5.1.2 The events of the postulated attack should be presented to law enforcement or other offsite armed responders, sequentially and in real time, by an exercise controller.

- Such presentation may include use of messages, scripts, or graphics to relay information such as officer reports, camera observations, intrusion/door alarms, etc.

5.1.3 If personnel are pre-staged, develop appropriate time delay criteria to be used before allowing individuals to begin "play."

- Delayed individuals should wait in an area away from any active "play" activities and related communications.
- Where possible, actual communication methods should be used to communicate with pre-staged individuals.

5.1.4 The IC should direct measures to control access and protect the TOC.

5.1.5 The site should dispatch to the TOC a liaison from security and operations to interface with the IC, and representatives from local and regional LE. The conduct of escort-based missions may require added support from operations and/or security.

5.1.6 Actions directed by the IC and/or LE, such as road closures, evacuation of the public located near the site, and augmentation of resources, should be simulated.

5.1.7 Ensure that drivers of responding vehicles from offsite agencies know site access routes, entry requirements and destinations. These should reflect procedural guidance or agreed upon protocols (including Identify Friend or Foe), unless the exercise scenario extent-of-play dictates otherwise.

5.1.8 Exercise play should include a mission to simulate movement from the TOC to the OCA and PA.

5.1.9 In-field/on-scene controllers must be knowledgeable in the functions that they are controlling (e.g., security actions being controlled by security personnel).

- Field controllers should have a means to communicate with the Exercise Manager and other required locations/individuals.

5.1.10 Controllers should closely monitor the formulation and delivery of instructions to the plant staff and offsite armed responders (e.g., plant page announcements, pager text messages, etc.).

- These are the messages that provide direction concerning movement of personnel, and associated cautions and constraints.

- Messages contained in procedures may be modified as needed to reflect the exercise extent-of-play.

- Controllers should be prepared to direct or deliver messages as necessary to ensure exercise continuity.

6 TABLETOP EXERCISE

6.1 Prior to conducting an initial LSD, a TTX should be conducted.

- Representatives from the licensee and responding LE agency, State, and Federal agencies should be invited to attend the tabletop.

- The TTX is beneficial for identifying potential problem areas, defining protocols, and achieving aligned expectations.

- Typical TTX participants are the key personnel from various disciplines (e.g., site security, operations, emergency preparedness, and radiation protection; LE command, tactical teams, and dispatch) and levels within the organizations (e.g., executives, mid-level supervision, first-line supervision, and some rank-and-file members).

6.2 Licensee should utilize Attachment 2, "Recommended Guidelines for Tabletop Exercise," of Appendix A, for preparation and execution of a TTX. The frequency of recurrence should be agreed upon by the law enforcement or other offsite armed responders relied on for contingency response, including any supporting offsite agencies.

6.3 TTX participants should include, at a minimum:

(1) Law enforcement or other offsite armed response executives (e.g., Chiefs, Sheriffs, Federal Bureau of Investigation (FBI) Field Office Special Agents in Charge) or their designated representatives (e.g., Operations Commanders, Chief Deputies, FBI Field

Office Assistant Special Agents in Charge) for agencies that would provide tactical teams or incident command staff to a significant, real-world event at the site;

(2) law enforcement or other offsite armed responders' tactical team commanders; and

(3) licensee personnel who are the subject matter experts on security, emergency preparedness, operations, and radiation protection.

6.4 The licensee should ensure that a TTX is conducted at the implementation of a LECR and when more than 25% of law enforcement or other offsite armed responders' executive participants change (e.g., due to retirement, promotion, etc.).

6.5 The licensee should ensure that a TTX is designed to:

(1) validate whether existing policies, procedures, and interagency/inter-jurisdictional agreements are sufficient for contingency response;

(2) familiarize responding law enforcement or other offsite armed responders with important concepts (e.g., implications of site focus changing from individual safety to public health and safety, how response fits into contingency response, and applicability of response paradigms, deadly force considerations, etc.) and current or expected capabilities or actions related to a sabotage attack;

(3) identify the appropriate tactical teams, focus areas, and resources necessary for future information transfers and familiarization and exercise activities under the licensee's contingency response plan;

(4) ensure law enforcement and other offsite armed response tactical teams have sufficient, accurate information for planning and executing tactical missions to interdict and neutralize the DBT adversaries in the plant OCA, PA, and power block; and,

(5) identify and test viable primary, secondary, and tertiary communications systems and protocols for drills and exercises with law enforcement and other offsite responders.

6.6 The licensee should ensure that TTX and LSD action items are tracked, dispositioned, and captured as lessons learned when appropriate. The licensee should use the results from the tabletop exercises are used to update and validate the LECR.

ATTACHMENT 1 TO APPENDIX A
RECOMMENDED LIMITED-SCOPE DRILL OBJECTIVES

LECR Limited Exercise Objectives

As previously noted, A LECR is a law enforcement developed and controlled plan. LECR is just one label for the plan, or set of plans, that law enforcement or other offsite armed responders may develop to guide its contingency response to a power reactor site. When a licensee relies on law enforcement or other offsite armed responders to interdict and neutralize the DBT adversary, the licensee should align its SCP with whatever law enforcement or other offsite armed responders calls its response plan(s).

Objective	**Performance Attributes**
1. Demonstrate the ability to implement the LECR for responding to a DBT attack.	Timely implementation of on-site LECR response actions.
2. Demonstrate the ability to make initial notifications to LE agencies during a LECR event.	Timely notifications are made to LE agencies as specified within the LECR.
3. Within the Tactical Operations Center (TOC), demonstrate the ability of security personnel to coordinate response actions among themselves and with the Incident Commander (IC) and LE personnel.	Discussion, decision-making and communication related to: • Threat type, location, progression, and changes to protective strategies • Dissemination of appropriate protective measure instructions to licensee on-site personnel • Entry and/or staging areas for LE • Coordination and deployment of LE resources • Plant status, damage assessments, personnel casualties, and tactical response priorities • Movement of licensee personnel to perform Credited Operator Actions, Damage Control Measures, or other critical tasks in the active- or post-attack environment • Identifying Friend or Foe (IFF)
4. Demonstrate the ability of site personnel to coordinate with the IC for deployment of on-site personnel and offsite tactical response in an active- or post-attack environment.	Discussion, decision-making and communication related to: • Initial accident assessment and mitigation • Use of staging areas for tactical response personnel and vehicles • Deployment of tactical response personnel.

Objective	Performance Attributes
5. Demonstrate the ability to implement appropriate radiation protection measures for offsite armed responders.	Discuss and/or implement appropriate radiation protection measures.
6. Demonstrate the ability of the site to support operation of a TOC.	Discussion, decision-making and communication related to: • Activation of a TOC • Accessibility by offsite armed responders • Dispatch of site personnel to the TOC to serve as liaisons to site security personnel • Availability of the contingency response tool or other site and plant layouts or other aids that the TOC staff might need to effectively manage the LE responses • Communications with response teams.
7. Demonstrate the ability to assess the impact of the attack on the plant physical security, and to identify and implement compensatory measures if needed.	• Security management should assess the effects of the attack on the ability to control access (to both the site and the protected area), maintain defensive positions (officer casualties, damage to protective enclosures, etc.), and operate security-related equipment. • Measures should be developed to restore physical security, including use of local LE agency personnel and resources. These measures should be coordinated with the TOC.
8. Demonstrate the ability to mobilize the tactical response teams in an active- or post-attack environment.	Discussion, decision-making and communication related to: • Status of the plant and potential for core damage/threat to public • Selection of a method(s) to protect operations movement/safe passage • Mobilization instructions provided to responders (e.g., routes, escorts, and exclusion areas; proceed directly to facilities; do not detour to inspect damage, etc.) • Crime scene preservation.

Recommended Objective	Performance Attributes
9. Demonstrate the ability of the IC to coordinate in-plant and on-site response actions with site security and within the TOC.	• Effective interface between security supervision and the IC, including their roles, responsibilities and authorities as conditions change. • Response personnel adhere to movement and other restrictions imposed by the IC, safety, and LE decision-makers, (e.g., stay clear of perimeter zones, definition of free movement areas, special identification, two-person line-of-sight rule, use of escorts, etc.).
10. Demonstrate the ability of the TOC to utilize a coordinated offsite response to support the conduct of Credited Operator Actions in both an active- or post-attack environment (Supports Adversary Interference Precluded Time (AIPT) analysis)	• Effective coordination between on-site and offsite response capabilities. • IC effectively utilizes the TOC to plan and execute Credited Operator Action based missions. • Effective coordination between site operations and both on-site and offsite armed responders in execution of operations-based missions.
11. Identify and implement improvements based upon exercise-based learnings.	• Effective utilization of the site-based corrective action process • Effective use of the interface between the on-site security force and offsite response agencies for capture and address of exercise-based improvement opportunities.

ATTACHMENT 2 TO APPENDIX A
RECOMMENDED GUIDELINES FOR TABLETOP EXERCISE

1. INTRODUCTION

1.1 The LECR TTX provides a facilitated learning environment for key licensee personnel, and law enforcement or other offsite armed response to review and discuss their respective roles and responsibilities.

- The TTX helps ensure the practicality and effectiveness of the licensee's LECR plan. Specifically, the TTX permits the various organizations to gain an understanding of each other's needs and priorities when responding to a hostile action which would require activation of the LECR.

- For example, the TTX can provide law enforcement and other offsite armed responders with a perspective on the plant operations, including delay systems and security features for protecting immediate access to target sets and providing sufficient time for response, immediate radiation hazard concerns, and protection of equipment important to safety.

- Likewise, the licensee will gain an appreciation for law enforcement and offsite armed response requirements and the operational aspects of the Incident Command Structure (ICS).

- Therefore, it is important that the structure and conduct of the TTX encourage a free exchange of viewpoints and concerns among the participants.

1.2 In order to enrich the learning environment, scenarios used in a TTX should be sufficiently different from previous TTX scenarios.

- A TTX facilitator(s) will use a scenario to lead participants through a series of postulated attack and post-attack events in a logical sequence.

- The TTX facilitator should pause after each event to elicit discussion from the participating decision-makers.

- For example, after presentation of the initial attack event, station security would explain its responses.

- The facilitator will then seek input from, in order, site personnel, law enforcement or other offsite armed response.

1.3 Details concerning implementation of a TTX are presented below.

2. DISCUSSION TOPICS

2.1 The overarching objective of the TTX is for the participants to achieve mutual understanding of each organization's roles, responsibilities, priorities, and actions when responding to an event. This understanding should contribute to a successful response

during the LSD. The Exercise Manager should consider the following topics for inclusion in the tabletop agenda.

- Method(s) used by the site to notify law enforcement or other offsite armed first responders of a threat and/or attack.
- Method(s) for subsequent dissemination of this information among offsite response organizations.
- Initial site safety/security actions in response to the DBT event.
- Initial law enforcement and other offsite armed responder actions upon notification:
  - Site access requirements for law enforcement or other offsite armed responders
  - Staging and/or reporting location(s) of law enforcement and other offsite armed responders
  - Communications and coordination with Incident Commander (IC) and site security

2.2 Establishment of the Tactical Operations Center (TOC):

- Who oversees the overall response, and how would transitions in command and control take place as the scenario evolves?
- Key support personnel reporting to the TOC and their respective functions
- How would offsite armed responders obtain turnover from, and integrate with, the site response?
- How will IC communicate and coordinate with on-site decision-makers?

2.3 Radiation protection provisions for law enforcement and other offsite armed responders to the site

2.4 Primary and backup means of communications between and among licensee safety/security personnel, the operation staff, law enforcement and other offsite armed responders, and any other emergency responders in the field and the TOC.

2.5 Coordination and decision-making related to:

- Ensuring that the TOC understands operational priorities for operation of functional equipment or restoration of damaged plant equipment
- Prompt movement of on-shift personnel to support plant stabilization, implementation of coping strategies, and/or cool down

2.6 Crime scene preservation

2.7 Coordination and addressing national media that may not be familiar with the local emergency preparedness plans/procedures/processes including FBI establishing temporary no-fly zones as defined within the site's SCP.

3 PREPARATION

3.1 The licensee should involve representatives from LE agencies and other first-responder organizations in the planning for the TTX. The offsite official who will serve in the capacity of the IC should have a role in preparation activities, including selecting participants, establishing discussion topics and objectives, and designing the scenario

3.2 The following TTX planning elements should be jointly determined:

- Date, time, and location
- What individuals from the site and key offsite response organizations will be invited to participate in the TTX
- Method(s) and responsibilities for inviting identified participants

3.3 Develop a simple, straightforward scenario that postulates an attack on the plant and consequences that require law enforcement or other offsite armed response and supporting resources. Review the scenario with representatives of key offsite response organizations to ensure that it promotes the desired range of participation. Suggested outcomes from this activity are to:

- determine what the agencies perceive as their role and extent-of- play, given the scenario.
- determine what the agencies want to learn from the TTX as a guide for the facilitator.
- determine which law enforcement and other offsite armed agencies and supporting agencies will have a lead and supporting role at different stages of the timeline.
- provide law enforcement and other offsite armed agencies the opportunity to think about their individual extents-of-play as the tabletop scenario evolves and how the command structure may change.
- establish ownership, among key offsite participants, of respective roles in the TTX.

3.4 Determine the room layout for the TTX.

- Thought should be given to locating the various organizations in the room to achieve maximum interaction and communication among key participants.
- For example, the IC and other key first response organization representatives will be located together at one table to represent the TOC.
- The room arrangement should facilitate communication between this location and initial on-site response personnel (i.e., on-site security).

- Site liaison personnel should be located at the TOC table to facilitate communication and understanding of plant information.

3.5 Set up the TTX area prior to the participants' arrival. Each table should have a sign, readable by all participants, that identifies the represented organization. A name and position placard should identify individual participants.

3.6 Observers and other non-participants should be in peripheral areas of the room so as not to interfere with participant interaction. A nearby break-out location may be designated for security personnel in the event safeguards discussions become necessary.

3.7 Depending on the size of the room and how far participants are situated from one another, a sound system and microphones may aid discussion.

4 CONDUCT

4.1 Each participant should be provided with a diagram of the TTX facility layout that identifies the participating organizations. They should also be provided with a list of all participants, their titles, and the organizations they represent. Designate a non-participant to take notes of the discussion and record key points and "parking lot" issues.

4.2 The lead facilitator should have the participants introduce themselves - participants should state their name, organization, and a brief statement of their role. The lead facilitator should review the rules for discussion of Safeguards Information (SGI).

4.3 The lead facilitator initiates the scenario by stating the initiating conditions and events and soliciting expected response actions from site personnel. This segment would include the process of threat identification and initial notifications to licensee on-site personnel and law enforcement and other offsite armed first responders. A short break may follow this segment to allow the notified organizations to review their response actions (at their respective tables) and prepare to present them to all TTX participants.

4.4 The facilitator(s) advances the timeline of the scenario segment by segment, soliciting response actions of each participating organization. As necessary, the facilitator(s) should prompt discussion concerning:

- Information requirements of each organization and how communications will occur among facilities and organizations.

- Active- and post-attack coordination necessary to allow movement of on-shift personnel and deployment of offsite response assets.

5 CRITIQUE AND FOLLOWUP

At the conclusion of the TTX, the lead facilitator should request that each table conduct its own critique and identify a summary of lessons learned and any items requiring further review and/or corrective action.

- In particular, participants should be asked to focus on issues that may have impeded effective LECR implementation.

- The lead facilitator should then ask the lead individual from each table to present the critique results to all participants.

- The designated note taker should record critique items and issues on a display visible to everyone.

- After presentation of each table's critique, observations should be solicited from any observer.

Response Validation Options	Benefits	Challenges/Limitations
Tabletop Exercise	• Can validate whether existing policies, procedures or interagency/inter-jurisdictional agreements are sufficient for and complementary to the implementation of the LECR; if they aren't, a TTX can facilitate revisions or the development of new policies, procedures, or agreements. • Having a TTX would be consistent with the Homeland Security Exercise and Evaluation Program (HSEEP) building-block approach. • Discussion-based event that enables participants to determine whether the LECR works conceptually, before actual resources are applied. • Valuable for familiarizing site and responding LE personnel with concepts and current or expected capabilities or actions • Helps to identify strengths and shortfalls and achieve changes in approaches or methods, when necessary • Participants can discuss issues in detail and develop decisions through a slow-paced problem-solving process.	• Outside influences that would be present during an actual event, or operational-based exercise, may not be addressed (e.g., onsite environmental conditions and hazards, diversionary events, human performance issues). • Primarily focuses on strategic, policy-oriented issues. • Provides only a high-level estimate of the current potential for success of the LECR. • Not all relevant personnel, especially actual operational elements, will take part in the exercise. • Because participation is limited, and actions are notional, operational or tactical considerations and lessons learned are not realized; considerable uncertainty remains regarding the skills, available resources, and actual capabilities necessary for executing the plan(s). • Outcomes and lessons learned may be limited to the participants and participating agencies, which could limit the benefit or utility of the TTX to other representatives from the broader offsite incident management system elements (e.g., emergency preparedness, fire, medical, radiation protection). • May need to clear all participants for access to Safeguards Information and ensure only cleared individuals and equipment are allowed in the TTX venue • Success of the event usually based on the skill and effectiveness of the facilitator
Tabletop Exercise	• Discussion topics involve multiple functions and considerations (e.g., communications, staging	

Response Validation Options	Benefits	Challenges/Limitations
	areas, coordination, command and control, public health and safety priorities, paramilitary tactics, use of force, casualties, etc.). • Participants are key personnel from various disciplines (e.g., site security, operations, emergency preparedness, and radiation protection; LE command, tactical teams, and dispatch; and potentially even fire and medical) and levels within the organizations (e.g., executives, mid-level supervision, first-line supervision, some rank-and-file members). • Relatively inexpensive and simple to plan and execute; lasts 4-6 hours; can be conducted at an offsite location	

Response Validation Options	Benefits	Challenges/Limitations
LSD	• Validates plans, policies, agreements, and procedures validated conceptually during the TTX • Operations-based event that can help to clarify roles and responsibilities, identify gaps in resources needed to implement plans and procedures, and improve individual and team performance • Improves tactical teams' familiarization with sites' power blocks, especially locations of safety-related equipment • Facilitates joint tactical planning and coordination • Tactical teams will gain some familiarity with dosimetry since they will need to enter the Radiological Controlled Area to familiarize them with safety-related equipment therein. • Induces LE to review site-specific information (e.g., the Contingency Response Tool) to plan and execute tactical operations • Enables tactical teams to conduct the three basic types of missions: defend, recapture and escort	• Exercise environment does not simulate several important conditions that would likely be present within the first 2-4 hours of an attack o Lack of adversaries to create the non-permissive environment in which site and LE personnel would be expected to operate o Lack of interaction with broader incident management system elements (e.g., incident command; non-law enforcement entities like fire, medical and radiation protection) o Lack of a Tactical Operations Center and accompanying elements, such as command and control and communications • More effective when tactical teams have access to information while they are inside the power blocks, which can lead to artificialities (i.e., having site staff accompany teams when no plans exist to do that during an actual response) or the need to issue portable electronic devices • Requires access to OCA, PA, VA and the Radiological Controlled Area, the latter of which necessitates additional training and can increase the length of the training day • Can involve significant site resources to provide escorts for LE at a 5-to-1 ratio (assuming LE enters vital areas for familiarization) • Involves pre-planning with the Contingency Response Tool (i.e., Safeguards Information (SGI)) or other site-specific information, which may require more SGI-accredited computer equipment than is normally available

Response Validation Options	Benefits	Challenges/Limitations
LSD	• Exposes tactical teams to several real-world stressors inside sites' power blocks in a permissive environment (e.g., heat, noise, radiation, interior complexity of site, communications challenges) • Provides opportunities for site escorts to engage in dialogue with LE tactical operators while moving through the plants (e.g., to point out security features, environmental hazards, convey tactical lessons learned during site contingency response training events, etc.) • May be able to test the same communications capabilities that would be employed during a real-world event (i.e., site radios used when offsite radios are not permitted or are not effective)	• Need to clear all participants for access to SGI, ensure the event includes only cleared individuals and equipment, and that participants always maintain control of SGI or portable devices • Potential for participant injury during physically demanding tactical training which could result in liability to the owning utility • Actions/behaviors by LE personnel, with minimal to no nuclear power plant experience, could inadvertently result in disruption of, or damage to, electrical generation or critical equipment, resulting in a plant shutdown. • Need exercise evaluation guides and a limited number of exercise controllers (from the site) and evaluators (from LE) to ensure plant safety and derive the most benefit from this event • Involves 1-3 hours of participant briefings (e.g., plant status, Safeguards Information, radiation safety, etc.) that can reduce the amount of time available for the exercise; if moved to the day prior to the exercise, participants and support staff would need to make an additional commitment.

APPENDIX B
CONDUCT OF LAW ENFORCEMENT AND OTHER OFFSITE ARMED CONTINGENCY RESPONSE FORCE-ON-FORCE EXERCISES

1. PERFORMANCE EVALUATION PROGRAM

1.1 Licensees should develop, implement and maintain a Performance Evaluation Program that is documented in procedures and describes how the licensee will demonstrate and assess the effectiveness of their physical protection program implementing the safeguards contingency response (i.e., protective strategy), including the capability of law enforcement or other offsite armed response relied upon to carry out interdiction and neutralization functions during safeguards contingency events.

- Acceptable methods for conducting tactical response force-on-force (FOF) exercises for assuring and demonstrating the effectiveness of law enforcement or other offsite armed responders to interdict and neutralize the design-basis threat (DBT) adversary are described in this guidance.

1.2 A licensee that relies upon law enforcement or other offsite armed response to interdict and neutralize the DBT adversary should conduct tactical response FOF exercises designed to demonstrate and assess the effectiveness of the licensee's physical protection program that includes law enforcement or other offsite armed response to contingency events.

- These drills and exercises are vital components of a comprehensive training program that enables the offsite responders to gain experience and demonstrate performance of tactics to effectively interdict and neutralize the DBT adversary and perform response tasks and activities within the contingency response plan.

2. TACTICAL RESPONSE FORCE-ON-FORCE EXERCISES

2.1 The objectives should be to:

- provide opportunities, within a permissive environment, for law enforcement or other offsite armed response tactical teams (or elements) to plan contingency response, conduct tactical operations with differing environments inside the plant's owner controlled, protected, vital, and radiological controlled areas;

- introduce law enforcement or other offsite armed response tactical teams to several real-world stressors (e.g., hostile environment, heat, noise, radiation, interior complexity of site, communications challenges); and

- identify and document law enforcement and other offsite armed response command and control and communications capabilities and incorporates those depictions into the law enforcement contingency response plan (LECR).

2.2 Licensee FOF exercises (fully integrated, tactical, and limited scope exercises) should be designed to challenge the site protective strategy against elements of the DBT and ensure that each participant demonstrates the requisite knowledge, skills, and abilities.

- Therefore, licensees relying on law enforcement or other offsite armed response to carry out the interdiction and neutralization of the DBT adversary should ensure that exercises meet these objectives.

- Participation in tactical response drills and FOF exercises are training activities that focus on maintaining and improving the knowledge, skills, and capabilities of the law enforcement or other offsite armed response teams and they are part of the ongoing training to assure effectiveness of the licensee's safeguards contingency plan (SCP) and the LECR.

2.3 The scope of exercises conducted for training purposes should be determined by the licensee and law enforcement or other offsite armed responders; address physical protection system and programmatic elements (e.g., detection and assessment, communications, delay) capabilities; and may be limited to specific portions of the LECR implementing the site protective strategy.

- Exercise plans and documentation must clearly identify the elements to be evaluated.

- The exercises provide a structured process to train personnel and evaluate key elements of the law enforcement or other offsite armed response by focusing on specific aspects of the strategy without conducting a fully integrated FOF exercise.

2.4 The structure of the exercise must ensure that it provides a credible, realistic, and comprehensive test of the elements of the LECR objectives that the exercise was designed to achieve.

- law enforcement or other offsite armed response tactical response FOF exercises and associated contingency response training should be conducted under conditions that simulate, as closely as practicable, the site-specific conditions under which each member of the security organization will, or may be, required to perform assigned duties and responsibilities.

- The exercise and scenarios used should ensure the satisfaction of the key contingency response elements addressed in this section of the regulatory guide (RG).

- Other licensee physical protection program elements, such as insider mitigation, cybersecurity, access authorization, and inspection, testing, and maintenance of physical security structures, systems, and components (SSCs) should also be considered in the development of exercise plans and scenarios to test, evaluate, and improve these areas.

- Section 5 of this appendix gives examples of these elements.

2.5 FOF exercises are an integrated response exercise that includes the participation of the law enforcement or other offsite armed response personnel executing the tactical operations against an opposing force with the characteristics and attributes of the DBT. FOF exercises are designed to train and/or evaluate law enforcement or other offsite armed responders on the complete implementation of interdiction and neutralization functions of the licensee’s contingency response and the evaluation and improvement of that LECR against the characteristics and attributes of the DBT adversary.

2.6 FOF exercises may be characterized as:

- a fully integrated FOF exercise,
- a tactical response FOF exercise, and
- a limited scope FOF exercise.

The FOF exercises should be used to exercise both licensee and the law enforcement (LE) personnel identified in the LECR to perform interdiction and neutralization functions. For each FOF exercise, the licensee should document all participants, including LE armed responders.

- Fully integrated FOF exercises. These exercises consist of a planned response effort across various plant disciplines (e.g., local law enforcement agency (LLEA)), security, plant operations, and emergency preparedness) to minimize or mitigate the threat.

- Security response FOF exercises. These exercises involve the full security response force and a mock adversary force without a planned response effort across various plant disciplines (e.g., LLEA, plant operations, and emergency preparedness) and focus primarily on security response.

- Limited scope FOF exercises. These exercises focus on the security response by using the minimum number of members of the response force and the mock adversary team sufficient to execute the scenario being tested. These should be a credible, realistic, and thorough test of a portion of the site protective strategy and evaluate the key security program performance elements bounded by the DBT. The exercise provides scenario controls and exercise controllers and includes a post-exercise critique and required exercise documentation.

2.7 The licensee should ensure that at least one fully integrated FOF exercise is conducted annually or more frequently, where the need is indicated, to ensure licensee and LE armed responder proficiency in implementing the LECR for an actual safeguards contingency event. This would include LE's ability to interdict and neutralize the DBT adversary. The following are consideration of the benefits and challenges/limitations of a fully integrated FOF exercise:

2.8 Defining Participation

2.8.1 Licensee personnel assigned duties and responsibilities required to implement the SCP and licensee protective strategy should participate in at least one tactical response drill quarterly and one FOF exercise annually. In addition, a licensee relying on law enforcement or other offsite armed responders to implement the SCP and fulfill the physical protection interdiction and neutralization functions should make available periodic training to law enforcement or other offsite armed responders who will fulfill the interdiction and neutralization functions for threats up to and including the DBT of radiological sabotage. Licensees should ensure that tactical response drills and FOF exercises reflect the LECR and role of responding law enforcement or other offsite armed response personnel and make these ongoing training opportunities available to assure effectiveness of the licensee's SCP and the LECR.

2.8.2 In accordance with 10 CFR 73.100(b)(4)(iv)(B), the licensee must satisfy the performance evaluation requirements in 10 CFR 73.100(g) for all armed response personnel, including law enforcement. Licensees must document the scenarios and participants for all tactical response drills and annual FOF exercises. Licensees are relieved from the training and qualification requirements related to law enforcement response personnel in paragraphs 10 CFR 73.100(c) and (e); however for law enforcement responders that participate in tactical response drills and FOF exercises, licensees should document those law enforcement participants.

2.8.3 When planning drills and exercises, personnel should be identified to fill each of the roles and response team duty positions and duty functions required to support the selected scenario and the type of drill or exercise being conducted.

2.9 Key Program Elements

2.9.1 For licensees that rely upon law enforcement or other offsite armed response to interdict and neutralize the DBT adversary the licensee should use, but is not limited to, the following elements of the LECR in developing scenarios for tactical response drills and FOF exercises to demonstrate an effective response.

- Responding with the number of law enforcement or other offsite armed response personnel. The law enforcement agency on which the licensee relies should have the required number of law enforcement response personnel to effectively implement the contingency response.

- Responding within the plant delay systems and appropriate law enforcement or other offsite armed response timelines. Law enforcement or other offsite armed response personnel have adequate time to perform tasks and activities to interrupt, interdict and neutralize the DBT adversary in advance of the adversary timeline to complete defeat of plant delay systems.

- Responding to implement tactical operations to defeat DBT adversary blocking measures and impeding force to prevent or delay law enforcement or other offsite armed responders to plant areas. Law enforcement or other offsite armed response personnel use appropriate protection and cover.

- Responding law enforcement or other offsite armed responders can protect the site from an adversary attack in accordance with the DBT and protect loss of target set components from sabotage by the DBT adversary force. Identifying potential tactical considerations along routes (e.g., DBT blocking force, improvised explosives, environmental hazards).

- Responding law enforcement or other offsite armed response with appropriate armament. Law enforcement or other offsite armed response personnel are equipped or have readily available the weapons and equipment necessary to execute their tactical operations.

- Responding law enforcement or other offsite armed response command and control structure. Law enforcement or other offsite armed response personnel have appropriate communication capabilities to ensure that decisions and

actions are coordinated and communicated in a timely manner to facilitate response. Law enforcement or other offsite armed response communications equipment used to the maximum extent practical; law enforcement or other offsite armed response Tactical Operations Center (TOC) established to document law enforcement or other offsite armed response radio communications capabilities and facilitate interoperable communications and route navigation.

2.9.2 To be an effective evaluation tool, each tactical response drill and exercise should include at least one of the program elements identified above. A FOF exercise should include all the elements described above. The following additional elements also contribute to the successful demonstration of the key elements:

- coordination and planning.
- command and control.
- communications.
- individual responder tactics.
- team response tactics.
- use of deadly force.
- alarm assessment and intrusion detection.
- weapons handling and proficiency.
- controller participation.
- post-drill briefing and critiques.
- integrated response (plant operations, Emergency Preparedness).
- deployment of responders and equipment.

2.9.3 Exercise Scenario Development

2.9.3.1 The effectiveness of a drill or exercise as an evaluation tool largely depends on the scenario development phase. Proposed scenarios should be designed to ensure that it adequately challenges the selected program elements. With a properly planned scenario, the critique and evaluation can provide meaningful insights into the effectiveness of the protective strategy and any enhancements or corrections that may be needed.

2.9.3.2 The scenarios should be designed to encourage open decision-making consistent with the protective strategy. In some cases, the scope of a drill may be more narrowly focused and not involve an adversary team. In those cases, only the relevant planning elements need be included. During scenario planning, attention to the key program elements is essential to the effectiveness of the drill or exercise as an evaluation tool. The design of the scenarios must ensure that they evaluate the effectiveness of the licensee's protective strategy. Since drills or exercise scenarios are developed based upon the licensee's protective strategy, they are typically considered Safeguards Information and controlled in accordance with 10 CFR 73.21.

2.9.3.3 The licensee should implement a process that ensures changes to the configuration of established equipment and systems related to target set components are considered in the licensee's scenarios developed for drills and FOF exercises. The scenario package(s) should ensure that the licensee has designed and developed drills and exercises that consider all modes of operation (i.e., operating at power, refueling, or other major maintenance activities). In addition, the licensee should consider the impact that various modes of operation have on the LE response, specifically, the impact that these modes of operation have in the following areas:

- law enforcement or other offsite armed responder timelines and positioning;
- impact of changes in the configuration of delay barriers;
- temporary modifications to the security plan to support activities that impact the safety/security interface;
- effects on fields of fire; or
- changes to target sets.

2.9.4 Identification of Target Sets

2.9.4.1 Drill and exercise scenarios should also be developed with the objective of interdicting and neutralizing the DBT adversary to prevent radiological sabotage by protecting target sets as a basis for the scenario. Target sets selected for a drill or exercise should pose the greatest challenge to the law enforcement or other offsite armed response. Target sets that have a small number of components, that are easily accessible, or whose component locations are in close proximity to each other should be an optimal choice for a drill or exercise scenario. Scenarios involving target sets generally can be the basis of improvements to physical protection systems and contingency response implementing the licensee's protective strategies that rely on the LECR.

2.9.4.2 The licensee may take credit for plant delay systems that function to delay DBT adversary access to the plant areas containing target sets that, if destroyed or disabled, would lead to radiological sabotage. The licensee identification of target sets is described in 10 CFR 73.100(b)(5), and guidance is described in RG 5.81.

2.9.5 Simulations and Artificialities

2.9.5.1 Drill and exercise scenarios should be developed to challenge the execution of the protective strategy during a variety of environmental and plant conditions. To replicate these conditions, it may be necessary to incorporate certain artificialities into the drill or exercise

scenarios. Plant conditions identified in the scenario may range from operating at power to refueling or other major maintenance activities.

2.9.5.2 Environmental conditions identified in the scenarios should include time of day or night, and, if possible, the drill or exercise should be conducted during the time identified to address relative daylight or darkness and various conditions of security readiness. If no acceptable artificialities are available for use or it is unsafe to incorporate the conditions into the drill or exercise scenario, a tabletop method may be used to simulate that condition, consistent with the licensee's site-specific analysis for how that specific condition affects implementation of NRC requirements.

2.9.5.3 The scenario may also need to include other artificialities to simulate actions and activities that cannot be performed for reasons of practicality and the safety of personnel and plant equipment. During scenario development, activities such as the use of firearms with blank ammunition and the use of mock explosive devices, and the presence of drill or exercise participants in certain areas, should be considered to ensure the continued safe operation of the plant and the safety of personnel. Drill and exercise scenarios should be developed to accommodate overall safety through the incorporation of acceptable artificialities to simulate the occurrence of these actions and activities (e.g., the inclusion of task times, timeouts, tabletop exercises). Additional discussion may be found in RG 5.74, "Managing the Safety/Security Interface."

2.9.5.4 Simulations and artificialities may apply to both licensee and law enforcement or other offsite armed responders and mock adversaries and should be thoroughly integrated and accounted for during the planning process. To enable controllers to properly inject simulations and artificialities into the scenario and oversee the actions resulting from them, the licensee's drill and exercise scenario matrix should incorporate specific guidance for simulations and artificialities. The licensee should minimize the number of simulations and artificialities in the development of scenarios to ensure that each scenario provides an accurate performance standard.

2.9.6 Cautions and Restrictions

Certain areas of the plant, such as the control room and areas where work is ongoing may be considered off limits to drill or exercise activity. Participants should receive this information at the drill or exercise briefing along with details of how the activities will be simulated or affected by these areas being off limits to drill or exercise activity. In addition, the following should be treated with special awareness during drill and exercise planning:

- areas with sensitive plant equipment;
- personnel safety;
- radiological controls;

- foreign material exclusion areas; and
- confined space areas.

2.9.7 Communications

The means of communication for the drill or exercise activity should be designated during the preparation phase. Planning for communication needs should consider plant operations, the on-duty plant personnel, the law enforcement or other offsite armed response participants, the controllers, and the mock adversaries, as well as communicating the conduct of the drill or exercise to onsite and offsite personnel.

2.9.8 Scheduling and Planning

2.9.8.1 Planners should ensure that the drill or exercise scenario maintains consistency with the DBT of radiological sabotage. The mock adversary force used in either FOF or licensee exercises must replicate, as closely as possible, the adversary attributes, characteristics, and capabilities of the DBT, and be capable of exploiting and challenging the licensee's protective strategy, personnel, command and control, and implementing contingency response.

2.9.8.2 The licensee should consider developing and maintaining a schedule that supports the drill or exercise plan to ensure the efficiency and productivity of drills and exercises. In schedule development, the licensee should consider factors such as projected station outage schedules, law enforcement or other offsite armed responders' availability, and FOF tactical exercise requirements.

2.9.8.3 An effective program schedule would provide a detailed listing of the following:

- type of drills/exercises to be conducted;
- when the drills/exercises will be conducted;
- key contingency response elements or evaluation standards to be satisfied by the planned evolution; and
- the participants in the evolution.

2.9.8.4 The licensee should consider use of a structured plan to assist in the coordination, execution, and documentation of activities associated with the drill and exercise process. The plan can provide consistency to the process and help ensure satisfaction of key contingency response elements or evaluation standards for implementing the performance assessment program requirements. The plan is also the foundation of the remainder of the drill or exercise documentation. The drill or exercise plan should address the following:

- drill or exercise specifics (number, date, shift/personnel involved, location).
- pre-notifications (operations, radiation protection, station management, etc.).
- safety briefings.
- radiological briefings.
- specific drill objectives or key elements evaluated.
- participants (players, controllers, adversaries).
- adversary characteristics (equipment, tactics, actions taken, target, etc.).
- scenario being used.
- sequence of events (event description, anticipated response, estimated timelines).
- development of a controller matrix (written scenario for controllers) to outline scenario events.
- simulations and artificialities to be considered or integrated into the evolution safety review.
- adversary briefings (providing details of the scenario, equipment used, routes, targets, etc., and allowing for intelligence gathering from an insider).
- controller/evaluator briefings (scenario, assignments, simulations, cautions, concerns, etc.).
- equipment consideration.
- initial plant/security status; and
- what LECR personnel tasks and activities are being tested.

2.9.8.5 In planning the drill or exercise, it is important that the licensee maintain the integrity of the process and the confidentiality of the scenario.

2.9.9 Command and Control of Drills and Exercises

2.9.9.1 Industry experience in the conduct of tactical drills and exercises as well as emergency preparedness exercises has demonstrated the need for a structured command and control process. A system of command and control is necessary to ensure maintenance of an environment free of the recognized hazards associated with tactical drills and exercises. The command and control system helps to ensure that the rules of engagement are followed, and hazards and

safety concerns are appropriately addressed. This structure includes the reporting relationship of all controllers to the lead controller.

2.9.9.2 All tactical drills and exercise activities must be conducted by exercise controllers and the exercise controllers should be under the guidance and supervision of a lead controller.

2.9.9.3 An exercise command and control system depends on a cadre of qualified personnel selected and specifically trained to conduct tactical drills and exercises. In addition to being trained to oversee exercises, controllers should receive training commensurate with the scope, complexity, and special nature of the activity. A controller's primary responsibility is ensuring safety during drill or exercise engagement. The controller organization should be structured in a manner that facilitates the control of all affected locations and the control and coordination of all events to be initiated during an exercise.

2.9.10 Controller Training and Qualification Process

2.9.10.1 Drill and exercise controllers should be trained and qualified to ensure that each controller has the requisite knowledge and experience to control and evaluate exercises. The following sections provide a basic overview of an acceptable process to ensure consistent development and implementation of controller training and qualification. These sections also describe the training feedback process to ensure continual improvement in both industry-wide and site-specific training programs.

2.9.10.2 The goals of the process are the following:

- establish a common baseline of controller knowledge, skills, and abilities.
- identify and respond to station and industry controller performance gaps.
- facilitate peer sharing of controller resources for exercise activities; and
- provide a feedback loop to support continual improvement in controller performance.

2.9.11 Controller Knowledge and Experience

2.9.11.1 Each controller should have the knowledge and experience to control and evaluate exercises/drills. This includes the ability to:

- provide timely and accurate information to drill players and participants to ensure consistent and orderly continuation of the drill or exercise in line with the scenario.
- evaluate the application of the no-play area (to include radiation boundaries) and control measures.
- evaluate tactical decisions and movements made by the LECR and the mock adversary force to include, as applicable, alternate avenues of approach, entry points, targets of opportunity, and control measures and tools required to facilitate entry.
- evaluate the application of the use of cover and concealment to include natural and fabricated defensive positions by all exercise players. This includes defensive positions and/or re-deployment, if required by the exercise.
- evaluate the tactical use of exercise weapons comprising their effective range and capabilities, including fields of fire.
- evaluate the application of target identification, acquisition, and engagement by players.
- evaluate the tactical use of hand-carried explosive devices on equipment and personnel and their effects upon detonation.
- evaluate the effectiveness of body armor employed by players and its ballistic protection during the exercise.
- evaluate the effectiveness of gas masks, or other supplemental gear, employed during the conduct of the exercise.

2.9.11.2 All controllers need to be aware of the entire exercise scenario, including the actions expected of the participant they are monitoring. The controller should evaluate actions that deviate from the expected scenario to ensure that the intent of the exercise scenario is being realized. In addition, licensees should also consider requiring that controllers have knowledge and experience in the following areas:

- the use and understanding of the dispersal and effects of chemical agents and smoke grenades.
- the gas mask used and its limitations.
- the overall procedure for conducting FOF exercises, including the use of Multiple Integrated Laser Engagement System (MILES) equipment.
- applicable site-specific delay barriers and movement timelines.
- the site’s policy on use of deadly force; and
- exercise and site safety procedures.

2.9.12 Training Design, Development, and Implementation

2.9.12.1 All controllers should complete controller training and any necessary requalification before participating as a controller in any drill or FOF exercise.

2.9.12.2 Licensees should develop controller training lesson plans and learning objectives for initial and refresher controller training. The controller training program should include, but not be limited to, the following:

- procedures, guidelines, and references.
- introduction/history.
- safety and safe drill play.
- communication (primary and alternate).
- terminology.
- command and control.
- providing acquired information to players.
- controller knowledge.
- position and exercise pace.
- rules of engagement and the use of force.
- use and effects of explosives.
- rules of conduct.
- MILES equipment and limitations.
- site exclusion areas.
- temporary breaks in drill execution.
- response team duties.
- critique process; and
- use and control of safeguards information.

2.9.12.3 The training should include site-specific information (e.g., industrial safety requirements, weapons handling safety requirements, radiological safety, delay barrier movement timelines, and use of deadly force). It should also include, but not be limited to, the following example scenarios and practical demonstrations related to controller activities and calls:

- drill timeline coordination (situational awareness and proper cue injects).
- cover and concealment assessment.
- MILES equipment usage and safety.
- red (training) gun equipment usage, application, and safety.
- use of assigned equipment.
- target set equipment.

- licensee protective strategy.
- simulations related to gas masks.
- simulations related to smoke or other chemical agents.
- weapons/explosives capabilities and simulation methods; and
- safety control.

2.9.12.4 Controllers should maintain proficiency by routine participation in station FOF exercises. In addition to the described training, the selection of controllers for specific assignments should consider previous experience, skills, and physical abilities. For example, an adversary controller for a FOF exercise should have previously functioned in that position and have the physical capabilities to remain with the adversary force. The controller briefing for FOF exercises should include just-in-time training to remind controllers of specific situational calls, safety issues, and critical communications that they could encounter during the scenario.

2.9.12.5 The level of support needed for the conduct of a drill will typically be significantly less than for an exercise, depending on the complexity of the drill. The licensee may consider the following positions of responsibility and personnel when planning for drills and exercises:

2.9.12.5.1 Lead Controller - the exercise leader with an overall knowledge of security shift operations. This individual may be selected from the security staff or other organization as appropriate.

2.9.12.5.2 Controllers - designated individuals assigned to specific participants or areas that have the necessary training to observe, evaluate, and control the drill or exercise activities of their assigned participant or control area.

2.9.12.5.3 Mock Adversary Force (MAF) - replicates, as closely as possible, adversary attributes, characteristics, and capabilities of the DBT of radiological sabotage as described in 10 CFR 73.1(a) and is capable of exploiting and challenging the licensee's protective strategy, LE response, personnel, command and control, and implementing procedures. Appropriately equipped and trained mock attackers with the required physical abilities to engage the licensee exercise participants in an armed attack to test the licensee's ability to defend against the DBT. Within the control and safety parameters established for the exercise, the mock adversary team will perform the normal physical and tactical activities (i.e., movement, communication,

and carrying of simulated explosives and equipment) required to accomplish their assigned mission. To execute such operations and tactics, it is essential that mock adversary team members are trained in small-unit tactics and scenario planning. In addition, the mock adversary team should be provided with sufficient time to prepare for the mission (this includes scenario planning and rehearsal opportunities). Typically, the mock adversary force is from the licensee's security force, from other nuclear plants, or from local LE tactical response units.

2.9.12.5.4 DBT Insider - a knowledgeable individual who provides inside intelligence information to the mock adversaries. This individual could be a member of the plant technical staff, operations staff, or the security force. Before a drill or exercise, sufficient time should be allotted for the adversary team to gain intelligence information from the insider.

2.9.12.5.5 On-duty non-drill plant personnel, - plant personnel who are used during an FOF tactical exercise to ensure that the exercise meets all requirements identified in the site-specific physical security plan (PSP) and procedures.

2.9.12.5.6 Central Alarm Station (CAS)/Secondary Alarm Station (SAS) Participants – plant personnel stationed in the alarm stations who will perform CAS/SAS duties as drill participants during the drills and exercises. They will be briefed on drill conditions as required.

2.9.12.5.7 Security Drill or Exercise Players – LE responders who respond to the mock contingency event.

2.9.12.5.8 Plant Operations Participant(s) - individual(s) who would normally be assigned to a command and control function. Plant operations personnel should participate when significant simulated plant operations are expected from the scenario. Only plant operator actions listed in a target set should be used in determining whether an entire target set was compromised. If credit is taken for plant operator actions, an evaluation must be conducted to ensure that the actions can appropriately be credited under the postulated attack scenario and anticipated plant and environmental conditions.

2.9.12.6 Licensees should ensure that sufficient documentation has been retained to demonstrate that training has been completed for exercise controllers.

2.9.13 Mock Adversary Force Member Training and Qualification Process

2.9.13.1 Tactical response drills, force-on-force exercises, and associated contingency training must simulate as closely as possible those site-specific conditions under which each member of the security force will be expected to carry out assigned duties. Licensees should use the following training performance standards to help ensure that the mock adversary force (MAF) performance is credible and sufficiently well-trained. These standards facilitate successful MAF participation in realistic challenges as a basis for effective evaluation of a licensee's contingency response performance capabilities during FOF exercises. This section provides a basic overview of an acceptable process to ensure consistent development and implementation of MAF training and qualification. This section also describes the training feedback process to ensure continual improvement in both industry wide and site-specific training programs.

2.9.13.2 The goals of the process are to:

- establish a common baseline for MAF knowledge, skills, and abilities.
- identify and respond to site and industry MAF performance gaps and generic issues.
- facilitate peer sharing of MAF resources for exercise activities; and
- support continual improvement in controller performance.

2.9.13.3 The following physical qualifications should be maintained by MAF members:

- Annual medical examination by a licensed physician to certify that the individual is physically fit and able to perform under high levels of stress in inclement weather and/or during strenuous physical exertions without undue foreseeable medical risks.
- Each MAF member should report any known or suspected change in health or physical capabilities that might impair his or her mental or sensory capacity and/or agility or otherwise impact their safe and effective performance.
- The MAF member should possess the mental, sensorial, and motor skills required to perform all assigned tasks safely and effectively. Medical qualifications should include (1) mental alertness and reliable judgment; (2) acuity of senses and ability of expression sufficient to allow accurate communication by

written, spoken, audible, or other signals; and (3) motor power, range of motion, neuromuscular coordination, and dexterity.

- After medical certification by a licensed physician, each MAF candidate should meet the physical fitness standards of being able to run (1) a mile in a maximum qualifying time of 8.5 minutes and (2) a 40-yard prone-to-run dash with a maximum qualifying time of 8 seconds.

- The MAF should be physically capable of performing or simulating the characteristics and capabilities of the DBT adversary in an effective and timely manner.

2.9.14 Mock Adversary Force Member Knowledge, Skills, and Abilities

2.9.14.1 The MAF replicates, as closely as possible, adversary characteristics and capabilities of the DBT and is capable of exploiting and challenging the licensee's protective strategy, personnel, command and control, and implementing procedures.

2.9.14.2 Each MAF member should have the knowledge, skills, and abilities to do the following:

- Demonstrate a thorough understanding of DBT weapons, including handheld automatic weapons, incapacitating agents, explosives, and hand-carried equipment, and their capabilities. Demonstrate qualifications, for example, consistent with the requirements applicable to an Armed Responder as provided in Section VI of Appendix B to 10 CFR Part 73. The licensee should ensure that site-specific requirements needed to ensure individual MAF member performance or participation in site activities have been completed prior to performance or participation in any site activity.

- Demonstrate competency in individual and team tactical movement under both day and night conditions and in various environmental conditions.

- Demonstrate tactical communication skills (e.g., radio discipline, use of hand signals) that include providing timely and accurate information to the controllers to ensure consistent and orderly continuation of the drill or exercise in line with the scenario. This includes demonstration of techniques for authenticating human assets (e.g., authentication code, color-coded identification).

- Understand the entire exercise scenario up to and including the DBT. This includes positioning and exercise/drill pace (timelines).

- Understand the application of the no-play area (to include radiation boundaries), areas described in Section 2.9.6 in Appendix B of this RG, and control measures.
- Implement adversary tactics, techniques, and tactical decisions to include alternate avenues of approach, entry points, targets of opportunity, and control measures and tools required to facilitate entry. This should include door breaching and dynamic room entries.
- Demonstrate the application of the use of topographical analysis (water, woodland, industrial) and tactical maneuvers in each of these environments, taking advantage of cover and concealment opportunities. This may include the use of smoke.
- Demonstrate the tactical use of drill/exercise equipment and weapons, including their effective range and capabilities (including specialized equipment and weapons).
- Understand target identification, acquisition, and engagement by players, including rules of engagement.
- Demonstrate the tactical use of hand-carried explosive devices and grenades on equipment and personnel and their effects upon detonation. This should include the placement of door charges and equipment charges.
- Understand the effectiveness of body armor employed by players and its ballistic protection during the exercise.
- Understand the rapid, violent, individual, and small-unit movement, maneuver, and attack characteristics.
- Understand the techniques to test/defeat detection and assessment sensors and barriers, including microwave (mono and biostatic), E-field, buried sensors (e.g., seismic), infrared (active and passive), and video motion detector.
- Understand the use, effects, and dispersal characteristics of chemical agents and smoke grenades.
- Understand the features of any gas mask being used and its limitations in a stressful environment.
- Understand operational planning including the analysis of a site protective posture and in planning a mission with available resources (e.g., collusion with an insider).
- Understand the differences between the various types of insiders and how to use each type of insider effectively to obtain intelligence information and collect data.
- Understand the use of MILES equipment.
- Understand red gun equipment usage, application, and safety.

- Demonstrate a thorough understanding of DBT firearms knowledge, including safety, marksmanship, and manipulation skills with all weapons described in the DBT, or that might reasonably be expected to be deployed. Training should include a course of fire to enhance proficiency to shoot on the move and while wearing a gas mask. Firearms training should also include manipulation and malfunction-clearing techniques, fire discipline, and precision-shooting techniques.
- Demonstrate firearms proficiency with all types of weapons that might reasonably be employed during FOF drills or exercises.
- Understand the function, design, and capabilities of applicable plant delay systems and delay capabilities and defeat task times.
- Understand the use of deadly force.
- Understand exercise and site safety procedures including procedures, guidelines and references, and the procedures for the use and control of safeguards information.

2.9.14.3 Mock Adversary Force Member Training Design, Development, and Implementation

2.9.14.3.1 The site adversary training program should build upon the following:

- The adversary force training, knowledge, and skills as described in 10 CFR 73.1(a).
- Rules of engagement; and
- Adversary characteristics as described in RG 5.69.

2.9.14.3.2 Licensees should develop MAF member training lesson plans and learning objectives for initial and refresher MAF training.

2.9.14.3.3 MAF training should include site-specific information, industrial safety requirements, weapons safety requirements, radiological safety, delay systems and associate delay and use of deadly force. It should also include example scenarios and/or practical demonstrations related to MAF activities such as the following:

- drill timeline coordination (situational awareness and proper cue injects).
- cover and concealment assessment.
- individual and team tactical movement.
- physical security systems and barriers.

- any specialized equipment.
- MILES equipment usage and safety.
- red gun equipment usage and safety.
- weapons/explosives capabilities and simulation methods; and
- safety control.

2.9.14.3.4 All MAF members should complete this basic MAF training before participating in a FOF exercise. Completion of the training should be documented. To ensure currency of MAF knowledge and familiarity with industry and station controller issues, MAF members should complete documented initial or refresher training within the 12 months preceding their participation in an annual FOF exercise. Additionally, MAF members should maintain proficiency by routine participation in station FOF exercises.

2.9.14.3.5 In addition to the described training, the selection of MAF members for specific assignments should consider previous experience, skills, and physical abilities. For example, a MAF member for an FOF exercise should have previously functioned in that position and should have the physical capabilities to remain with the MAF. The MAF briefing for FOF exercises should include just-in-time training to remind MAF members of specific situational calls, safety issues, and critical communications that they could encounter during the scenario.

2.9.15 Conduct of Drills and Exercises

2.9.15.1 Safety during the conduct of drills and exercises is a significant element of the security-training program. Regardless of the scale of the evolution, preparation, coordination, and control are key elements to the effectiveness of a drill or exercise. To ensure exercise safety and provide consistent and effective performance, the licensee should consider the following criteria when conducting drills or exercises:

- Weapons/Ammunition Safety—Weapons and ammunition safety is paramount. It is crucial that proper attention is given during exercise planning and performance to ensure that drill participants do not carry or have available live-fire weapons or ammunition. The adversaries and the response force team should use training weapons that are easily identifiable as such. Weapons should be marked so they can be easily identified as training weapons. Live-fire weapons should not be used during

drills or exercises. If a live-fire weapon is used, it should be rendered safe and incapable of firing.

- Exercise Participant Safety—The following criteria should be part of the safety briefing for exercise participants:
  - Physical contact should occur only after a participant has been disabled, surrendered, or neutralized and only with the approval of a controller.
  - No attempt should be made to disarm an opponent in any way.
  - All ascents and descents from elevated positions will involve a ladder, stairway, or other safe method.
  - There should be no jumping from one elevation to another.
  - All exercise controllers and participants will be briefed on the radiological and industrial safety restrictions and concerns.
  - Participants should monitor their own condition for overexertion.
  - Anyone who observes an injured or ill participant should immediately call a timeout, render assistance, and notify a controller/evaluator or call the CAS or SAS.
  - The lead controller should discuss plant and weather conditions before the start of each exercise and address limitations on running, jogging, or walking.
  - All participants should use personal protective equipment unless otherwise determined by a controller.
- Initiation and Termination - The lead controller should initiate the exercise with the concurrence of the on-duty security supervisor and operations shift manager/supervisor, if applicable. The initiation of the exercise should be communicated on appropriate radio frequencies and/or the plant paging system. The lead controller should conduct radio checks as appropriate to ensure that all controllers are prepared for the initiation or resumption of the drill or exercise. The exercise will be terminated by the lead controller when one or more of the following occur:
  - all adversaries are neutralized or have given up the mission.
  - a complete target set has been destroyed.
  - the lead controller determines that an actual condition exists that cannot be quickly corrected or is of such magnitude as to preclude the continuation of the drill.

- the lead controller determines a condition adverse to personnel or plant safety exists; or
- the lead controller directs that the exercise stops.

2.9.15.2 Participant Responsibilities - The licensee's briefing for participants on their duties and responsibilities associated with the exercise should include, but is not limited to the following criteria:

- Each participant is personally responsible for his or her safe conduct.
- Each participant should monitor his or her condition.
- Participants who hear an announcement to stop the exercise should immediately stop all exercise activity and maintain their position until they receive additional instructions.
- Participants will comply with all plant operations, security, and radiation protection requirements. The pre-exercise safety briefing will address radiation protection entry and exit procedures.
- All participants should follow controller commands and requests. Participants should maintain contact with their assigned controller. If during the conduct of the drill or exercise the participant identifies that there is no longer a controller monitoring the drill or exercise activity, then they should stop and contact the lead controller. The post-exercise critique should address differences in interpretations of scenario evolutions.
- After the conclusion of the drill or exercise and before the critique, all participants should have an opportunity to document their participation in the drill or exercise so that their actions may be discussed and reviewed in the critique process.

2.9.15.3 Rules of Conduct - The licensees should consider including the following rules of conduct as part of the briefing for participants on the conduct of the drill or exercise:

- Safety is paramount. The safety of participants, controllers/evaluators, plant personnel, and the plant should never be compromised.
- If identifying clothing or items such as armbands are assigned, participants should wear them at all times during the drill or exercise.
- Participants will follow all instructions given by a controller.

- Any participant may stop the drill or exercise for safety reasons and should ensure that information is promptly communicated to the lead controller. The lead controller should determine the resumption of the drill or exercise.
- If the drill or exercise is temporarily halted, all participants should stop at their locations, cease all firing and movement, and wait for direction.
- Once neutralized, a participant should immediately cease all firing, movement, and communications. The participant should remain in place until the drill or exercise is terminated or the controller directs otherwise.
- Alarm station operators and/or participants may not engage in pre-drill or pre-exercise intelligence gathering. Participants who attempt to circumvent the rules will be removed from the drill or exercise.
- The controllers/evaluators observing and evaluating the activity should determine all neutralizations. Training equipment, such as MILES gear, can be used to assist in this determination.
- At the conclusion of each drill or exercise, participants should ensure that all radiological boundary controls are intact and that security doors involved in the drill or exercise are secure.
- The announcement "this is a drill" should be transmitted immediately preceding the first drill activity once the drill window is opened. This announcement should also be transmitted periodically throughout the drill and before any drill event after a long period of inactivity.
- To be successful during an exercise, the MAF should perform or simulate all actions necessary (including placing simulated explosives at doors, gates, and inside the target areas). If possible, the MAF should perform or simulate all actions necessary (including placing explosives) at the specific location where the equipment damage is intended to occur. If the actual equipment cannot be reached, the MAF may provide specific detail as to exactly where it intended to perform the action (or place the explosive and the amount to be placed).
- On-duty security force personnel should not assist or impede the participants in any fashion unless the circumstance pertains to a safety-related issue or to a real security situation or response.
- Participants should observe the deadly force rules of engagement as authorized by federal or state law and as defined by station policy. In addition, Staff Regulatory Guidance Position 8.13, "Use of Force," of RG 5.75, provides further guidance regarding the proper use of force within the force continuum.

- At no time should drill or exercise participant(s) manipulate any plant component. It should be stressed that extreme caution is to be used near plant equipment. Backpacks, mock weaponry, and associated drill or exercise equipment should be kept clear of plant equipment.
- Controllers/evaluators ensure that drill or exercise participants do not voluntarily or accidentally touch plant equipment, controls, or instrumentation. If at any time inadvertent contact is made with plant equipment, controls, or instrumentation, the controller/evaluator should immediately notify operations of the incident.
- The MAF and the insider must replicate, as closely as possible, the specific characteristics or requirements detailed in the DBT.
- Sufficient time should be allotted for the MAF to gain intelligence information from the insider.
- The MAF's familiarity with the plant should consist of only what the force has developed through information obtained from the insider or from other sources of public information about the facility, such as tours of the facility, or observations from publicly accessible roadways and areas adjacent the site boundary.
- The MAF should begin the exercise from the point where they would first have the potential for identification by or interaction with the licensee's security program measures.
- The MAF must replicate as closely as possible the adversary characteristics and capabilities of the DBT in 10 CFR 73.1(a)(1). This means that the MAF will adhere to the equipment and explosive weight limitations detailed in the DBT.
- When penetrating barriers (i.e., fences, doors, walls, etc.), the mock adversaries' entire task time (e.g., set time, time to achieve stand-off distance, time to recover the stand-off distance, and traverse the barrier) should be factored into the act. Proper care should be given to personal safety and protection when making entry. If portable blast protection is used, this equipment may be considered as part of the equipment carried in by the adversary team.
- Incapacitation criteria detailed in the DBT for weapons such as fragmentation devices, smoke grenades, and distraction devices will be followed during the exercise.

3. CRITIQUE AND EVALUATION

3.1 When the licensee relies upon law enforcement or other offsite armed response to provide the capability to interdict and neutralize the adversary, the licensee's reliance on law enforcement or other offsite armed response may be considered successful or effective if

the adversary is detected, assessed, interdicted, and neutralized before causing radiological sabotage by successfully disabling all target set components within a single target set.

- A licensee may not take credit for actions or equipment that are outside of the predetermined target set for the purpose of determining the effectiveness of law enforcement or other offsite armed response to carry out their tactical operations to interdict and neutralize the DBT adversaries.

- The licensee should enter identified drill or exercise deficiencies that adversely affect or decrease the law enforcement or other offsite armed response and the physical protection program into the plant's corrective action program or training program and correct the identified deficiencies.

- Licensees should review the programmatic deficiencies for information that meets the protection requirements of 10 CFR 73.21 and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements."

3.2 Members of the law enforcement or other offsite armed response team should be evaluated on all aspects of response, including but not limited to timeliness, use of cover and concealment, tactical movement and firing techniques, assessment, and communication.

3.3 Alarm station personnel should be evaluated for assessment, communication, coordination, including law enforcement or other offsite armed response notification/coordination, and other aspects of their operations under contingency events.

3.4 The law enforcement or other offsite armed response team leader should be evaluated for performance in demonstrating command and control and making sound and timely decisions for direction of law enforcement or other offsite armed response personnel to interdict and neutralize the DBT threat.

3.5 Controllers should be evaluated for accurately assessing the individual and overall licensee and law enforcement or other offsite armed response to a contingency event.

3.6 The critique process is a crucial aspect of the drill and exercise program. This process involves evaluation of participant performance through specific critique criteria, participant self-assessment, and observations by controllers/evaluators. The critique criteria should support the evaluation standards and performance criteria identified for the scenario.

4. CRITIQUE AND EVALUATION MATERIAL

4.1 Each tactical response drill and FOF exercise should include a documented post-exercise critique in which participants identify failures, deficiencies, or other findings in performance, plans, equipment, and strategies.

4.2 Findings, deficiencies, and failures identified during tactical response drills and FOF exercises that adversely affect or decrease the effectiveness of the protective strategy and physical protection program should be entered into the licensee's corrective action program to ensure that timely corrections are made to the appropriate program areas.

4.3 The following criteria should be considered when developing critique material for drill or exercise evaluation purposes:

- Each position and participant should be evaluated.
- The ability of each participant to satisfy the performance criteria associated with his or her position should be evaluated.
- Criteria not evaluated should be indicated on the critique. Evaluators should consider using "NE" (not evaluated) instead of "NA" (not applicable).
- The form should indicate whether the individual satisfied the performance criteria.
- Any issues identified because of the individual's performance should be documented. Issues should be correlated to their respective evaluation standards.
- Controller/evaluator performance evaluation comments should be solicited.
- The critique material should give participants the opportunity to critique their own actions and to provide feedback on the drill or exercise.
- The critique should include an overall assessment of the success of the drill or exercise in meeting the key program elements identified.
- Security equipment performance and security system performance should be evaluated as it relates to the licensee's protective strategy.

4.4 At the conclusion of a drill or exercise, the lead controller should facilitate the critique. All controllers/evaluators, adversaries, and participants should normally participate. These critiques give the participants the opportunity to receive direct feedback from the controllers/evaluators. In addition, they allow the participants to provide direct input to the critique process.

- Structured critiques allow the participants to provide direct input to the critique process. The following format can be an effective means of performing critiques. The structure of the drill or exercise critique should ensure:
  - All participants in the drill or exercise are in attendance.
  - The scenario, including goals and objectives, is thoroughly reviewed with the participants as a group.
- Each participant and corresponding controller/evaluator who had an engagement during the drill or has pertinent feedback will summarize his or her actions and should consider the following when providing an action summary:

- If a participant took action that resulted in his or her neutralization or the neutralization of an adversary or adversaries, then the participant and controller report should provide specific details of the actions taken. The participant/controller information should include engagement distance, number of adversaries engaged, number of rounds fired and number of seconds, the probability of neutralizing the adversary (high, medium, or low), and if the neutralization(s) resulted from MILES.
- If a participant took action that resulted in friendly fire, then the participant and controller report should provide specific details of the actions.
- A controller/evaluator whose participant had no interaction with the adversary force and had no effect on the outcome of the drill or exercise should participate (provide lessons learned feedback) to the extent of his or her direct observation of the exercise or drill.
- A controller/evaluator whose participant was actively involved in the outcome of the drill or exercise and who interdicted the adversaries should concur with the player's comments if applicable. If the controller/evaluator does not concur, he or she should provide details.
- At the conclusion of critiques, the lead controller should review the results of the drill or exercise and discuss the positive and negative aspects of the activities.
- During the review of the results, participants should be asked for suggestions for correcting issues and concerns, and these suggestions should be discussed.
- As a conclusion to the critique, the lead controller should review the goals, objectives, and key program elements of the drill or exercise and discuss how each was or was not met.
- Any participant or controller/evaluator that identifies a deficiency in the licensee's protective strategy (e.g., equipment, system, or performance failure), regardless of whether that participant took action in the drill or exercise, should provide specific details during the critique.

5. DRILL OR EXERCISE DOCUMENTATION

5.1 The results of a tactical response drill or FOF exercise should be documented and entered into the licensee's corrective action program. The following information should be part of the drill or exercise documentation:

- controllers,
- MAF,
- scenario description,
- key elements and evaluation criteria in the drill,
- failures, deficiencies, or other findings in performance, plans, equipment, or strategies,
- actions taken on failures, deficiencies, or other findings,

- corrective actions (plant corrective action or training program) and the timeframe or priority given for resolution and identification of the individual responsible for resolution, and
- which participants took part in the exercise(s).

5.2 The following information should be part of the drill or exercise documentation, and is in addition to the information described in Staff Regulatory Position 5.21.1 of RG 5.75:

- date and time,
- drill/exercise number or another identifier,
- plant conditions, security system status, and weather conditions,
- program or process strengths identified, and
- whether the goals, objectives, and key program elements of the drill or exercise were met.

5.3 The drill-planning package developed for the evolution should be attached to the report. The licensee should protect deficiencies identified during a drill or exercise consistent with the requirements of 10 CFR 73.21.

5.4 Program element deficiencies should be entered in the licensee's corrective action program. After the final critique results are prepared, the licensee can determine the disposition of each deficiency. Identification of issues from the drills or exercises is only the first step in the corrective action process. Management should thoroughly review each deficient item identified and promptly develop and take corrective action. To ensure resolution of issues, the licensee should regularly review the corrective actions identified through the drill and exercise process and evaluate their effectiveness.

5.5 It is important that drill and exercise activities are properly documented to ensure appropriate levels of review and resolution of issues. Not all documents generated in the process of performing drills or exercises should be maintained as records. The licensee should retain the following documents:

- scenarios,
- participation records showing which security force personnel participated in tactical drills and FOF tactical exercises, and when law enforcement or other offsite armed responders implementing the LECR participated, records should show which law enforcement or other offsite armed response personnel participated in the tactical drills and FOF tactical exercises,
- completed critique material, including chronologies,
- final drill or exercise report, and
- resolution or proposed resolution of critique items.

5.6 The licensee should retain an attendance roster for all drill- and exercise-related trainings and briefings.

Response Validation Options	Benefits	Challenges/Limitations
Full-Scale Exercise with laser engagement equipment	• Includes elements from the LSD Benefits • Involves relevant incident management system elements (e.g., fire, medical, Incident Command Post, Tactical Operations Center, a site's primary or alternate Emergency Operations Facility) • Involves actual mobilization of resources (e.g., mobile command posts, tactical teams in full gear) • Decisions and actions occur in real time. • Exposes tactical teams to the maximum number of real-world stressors inside sites' power blocks (e.g., adversary and law enforcement or other offsite armed response weapons fire, heat, noise, radiation, interior complexity of site, communications challenges) • Necessitates sound tactical plans and movements • Laser engagement equipment provides realistic tactical stimuli to which LE team members can respond, instead of responding to verbal information or a written inject.	• Includes elements from the LSD Challenges/Limitations • Adds additional layers of complexity to the tactical response and limited scope exercise • Using controllers as adversaries vice an adversary team to maximize the training value for law enforcement or other offsite armed response participants (i.e., minimize the win-lose mindset individual adversary players may exhibit) • Having controllers or adversaries who are flexible enough to know when to engage law enforcement or other offsite armed response to accomplish training/learning objectives (e.g., to slow progress and maintain the exercise timeline, to penalize poor tactical movement) • Requires exercise controllers (from the site), evaluators (from LE) and possibly role players, and specialized training for each group to ensure plant safety and to maximize the benefit from this event • Significant exercise documentation (e.g., exercise evaluation guides, master scenario events list, communications plan, controller/evaluator, and player handbooks) • Has a significant logistics component, from exercise venue locations and security; to participant transportation, sustenance, and screening; to communications networks and protocols • May involve a Simulation Cell • Incorporating laser engagement equipment training, issue, testing and turn-in into an already full schedule

Response Validation Options	Benefits	Challenges/Limitations
Full-Scale Exercise with laser engagement equipment	• Can identify potential incidences of fratricide or lessons learned on how to avoid them in the future	• Typically involves 2-4 hours of participant briefings (e.g., laser engagement equipment operation, plant status, Safeguards Information, radiation safety, etc.) that can reduce the amount of time available for the exercise; if moved to the day prior to the exercise, participants and support staff would need to make an additional commitment. • Finding enough laser engagement equipment to outfit LE participants and select controllers

APPENDIX C
ADVERSARY INTERFERENCE PRECLUDED TIME

1. APPLICABLE RULES AND REGULATIONS

10 CFR 73.100(b)(3) states that: *"The physical protection program must be designed to prevent the release of radionuclides from any source from exceeding the dose reference values defined in § 53.210 of this chapter."*

10 CFR 73.100(b)(5) states that: "*The licensee must identify and document complete and accurate target sets…"*

10 CFR 73.100(b)(5)(i) states that: "*Preventative operator actions may be credited as target set elements when: sufficient time to implement exists; environmental conditions allow operator actions to be completed successfully; adversary interference is precluded; all equipment required for operator actions is available, dedicated, staged, and maintained; approved procedures exist specific to the task being performed; and training is maintained for proficiency of the credited operator action*."

10 CFR 73.100(b)(5)(iv) states that: "*The licensee must further identify achievable target sets through a site-specific analysis. Achievable target sets are those that are within the capabilities of the design basis threat adversary to compromise, destroy, or render non-functional; cannot be mitigated after adversary interference is precluded and prior to a release of radionuclides exceeding dose reference values defined in 10 CFR 53.210; and, if defeated, result irreversibly in exceedance of the dose reference values defined in 10 CFR 53.210."*

10 CFR 73.100(b)(6) states that: "*The licensee must identify and analyze site-specific conditions, including achievable target sets, that may affect the physical protection program needed to implement the requirements of this section. The licensee must account for these conditions in demonstrating compliance with the requirements of this section."*

2. ADVERSARY INTERFERENCE PRECLUDED TIME (AIPT) CONCEPT

AIPT can be a useful planning tool that helps licensees understand when adversaries are no longer considered a threat to operator movement to ensure mitigation strategies, if needed, are effective and timely to prevent a release exceeding the dose reference values defined in 10 CFR 53.210. AIPT also represents the shortest amount of delay that is required by 10 CFR 73.100(b)(4)(iv)(A)(*2*) when an applicant or licensee relies on law enforcement or other offsite armed responders to interdict and neutralize threats up to and including the DBT.

AIPT should be calculated in accordance with guidance in this appendix.

2.1 Licensees should consider that responses to their calls for offsite assistance during an attack could have one of two immediate objectives:

- interdict and neutralize all known adversaries, so site staff can take action to prevent or mitigate offsite radiological consequences without adversary interference (hereafter referred to as an adversary-focused mission); or

- protect site staff and associated equipment from adversary interference in limited plant areas when there isn't sufficient time to interdict and neutralize all known

adversaries before the site staff takes action to protect public health and safety and the environment (hereafter referred to as a plant condition-focused mission).

The determining factor between the two mission types is whether there is sufficient time for law enforcement or other offsite armed responders to interdict and neutralize all known adversaries prior to site staff taking action to prevent or mitigate offsite radiological consequences.

Some circumstances may provide time only for the planned offsite response force personnel to secure safety-related areas of a facility (e.g., the immediate areas surrounding personnel, equipment, and pathways necessary for a preventative or mitigative action), leaving adversaries in other locations of the facility for a subsequent, mutual aid force(s) to interdict and neutralize.

Licensees should ensure that law enforcement and other offsite armed response personnel that the licensees rely upon to interdict and neutralize the DBT adversary are prepared for both mission types.

Licensees should calculate an AIPT for each mission type. If the AIPTs differ, the longer one should be used as the bounding AIPT (i.e., the AIPT applicants and licensees use to screen target sets pursuant to RG 5.81). If it's unclear which target set leads to the longest AIPT, multiple target sets may need to be evaluated to determine the bounding AIPT.

2.2 Licensees should calculate an AIPT by identifying and adding the following five time elements:

1) Alarm Assessment and Communication Time	Alarm Assessment and Communication Time includes the maximum time it takes for the licensee to detect and assess threats up to and including the DBT of radiological sabotage and the maximum time it could take for the licensee to notify the responsible offsite response element(s).
2) Response Time	Response Time is the period from when the responsible offsite response element(s) receives the licensee's call for assistance until the necessary response resources arrive at the site or designated staging area.
3) Mission Preparedness Time	Mission Preparedness Time represents the time it takes for offsite armed responders to review avenues of approach, facility floor plans, and other relevant site information; receive timely and accurate threat information; and develop and rehearse a mission plan(s) prior to site entry.

4) Mission Execution Time	Mission Execution Time is the period from when offsite armed responders depart the mission planning and rehearsal location or arrive on site and begin their missions (if the responders traveled directly to the site) until all known adversaries are neutralized (i.e., for an adversary-focused mission) or site staff completes preventative or mitigative actions to maintain the site at, or return the site to, a safe condition (i.e., for a plant condition-focused mission).
5) Safety Margin	Safety margin time is a constant time that attempts to account for the uncertainties that may exist in the data or assumptions used to calculate an AIPT.

2.3.1 Once calculated, a licensee should round its AIPT up to the next half hour (e.g., 13¼ hours becomes an AIPT of 13½ hours, 13 hours and 37 minutes becomes an AIPT of 14 hours).

2.3.2 A licensee should recalculate its AIPT when any of the time elements used to calculate the AIPT increase. When any of the time elements used to calculate the AIPT decrease, a licensee may opt to recalculate its AIPT or maintain its original AIPT so that it does not have to reassess or revise its target sets or adversary delay time.

2.3 Although the AIPT calculation methodology uses five discreet time elements, the NRC is aware that a licensee's specific circumstances may not perfectly align with this model.

- For example, a licensee should be able to identify all five time elements when it calculates an AIPT for adversary-focused missions.

- However, a licensee that has trained and validated offsite armed responders to an extent that enables them to complete mission preparedness activities while traveling to a site, would essentially condense the timelines for response and mission preparedness to only the time needed for response.

- Because the basis and justification for a site-specific AIPT could vary significantly from one site to another, a licensee should fully document its AIPT development process and decisions and have them available for inspection.

2.4 To the extent practical, a licensee should use data derived from real-world emergency responses to site calls for assistance.

- Licensees should consider data from other real-world emergency responses by the same law enforcement or other offsite response entity to be the next best source of information.

    - Data such as notification and assembly times may be similar regardless of the emergency event.

- When suitable real-world data do not exist, licensees should use data derived from exercises or other sources.

- For example, instead of using real-world emergency-related travel times to the site or designated staging area (e.g., law enforcement (LE) Code 3 response times), licensees may have to obtain travel time data for another location in the vicinity of the site or staging area and then modify the time to account for the difference in location between the data's actual destination and the site or staging area.

- Licensees may also identify travel times using a route planning tool with real time traffic condition capability; licensees adopting this method for identifying the travel time component of response time should identify routes for the range of traffic conditions that typically exist between the response force starting location and the site or staging area, and then select the route(s) with the longest time(s).

- Another source from which licensees may be able to identify suitable Mission Preparedness and Mission Execution Times is from drills or exercises.

3. GUIDANCE FOR DETERMINING THE FIVE ELEMENTS

3.1 Alarm Assessment and Communication Time

3.1.1 Alarm Assessment and Communication Time has two components:

- the maximum time it takes the licensee to detect and assess threats up to and including the DBT, and

- the maximum time it could take for the licensee to notify responsible law enforcement or other offsite armed response personnel.

To the extent practical, when determining the maximum detection and assessment time component, licensees should review a site's actual sensor performance and alarm acknowledgment and assessment data and use the maximum time demonstrated by that data.

Actual sensor performance and alarm acknowledgment and assessment data are the preferred sources for the detection and assessment times because the data will likely account for detection or assessment delays, such as those associated with adverse environmental conditions, potential signal travel over substantial distances, real-world distractions for an alarm monitor, or multiple, simultaneous alarms (e.g., alarm stacking).

3.1.2 When real-world alarm sensor performance and acknowledgment and assessment data are not available (e.g., newly installed intrusion detection system with few or no actual sensor activations to date), licensees should use the maximum detection and alarm acknowledgment and assessment times that were established during performance-based testing of the intrusion detection system(s).

3.1.3 Licensees should use 15 minutes as the notification component of the Alarm Assessment and Communication Time, since that is the maximum period that a licensee has after declaring an emergency, pursuant to Appendix E to 10 CFR

Part 50, paragraph IV.D.3, to notify responsible state and local governmental agencies.

3.1.4. Under this construct, the Alarm Assessment and Communication Time becomes the sum of 15 minutes and the maximum detection and assessment time.

3.2 Response Time

3.2.1 Response Time represents the period from when law enforcement or other offsite armed response personnel receive a licensee's call for assistance until the necessary response resources or assets arrive at the site or designated staging area.

- Activities such as paging a tactical team, tactical team mustering, and travelling to the site or a staging area are all components of Response Time.

- A licensee should consider a response force's available modes of travel (e.g., land, air, water) and utilize the travel time for the slowest mode to inform the Response Time used for its AIPT calculation.

- If a licensee relies on more than one response force for interdiction and neutralization of the DBT adversary, then the licensee should use the longest overall response timeline to inform the Response Time used for its AIPT calculation.

3.2.2 A licensee should calculate Response Time using one of two methods.

- The preferred method is for a licensee to collect information from single incidents, each of which involves a response by the necessary offsite resources or assets to the site or designated staging area.

  Using this method is more reliable, because all of the response variables (e.g., weather, traffic, communications challenges, rationale for decisions) are consistent across each of the Response Time components, and the starting and ending points used to calculate Response Times will represent complete and actual response time performance on a given day.

- A less-preferable method would be for a licensee to identify the times for Response Time components (e.g., maximum call-out, assembly, and travel times) from different incidents or events, and then combine those component times to create an estimated Response Time.

  This alternate method will likely produce uncertainties in the final Response Time estimate, because conditions that increase the time for one component on one day may not exist or adversely affect other component times on different days. A licensee should confirm the accuracy of its Response Time estimate with a subject matter expert who is a member of the offsite response force before including the estimate in its AIPT calculation.

3.3 Mission Preparedness Time

3.3.1 Mission Preparedness Time represents the time that offsite armed responders need to review avenues of approach, facility floor plans, and other relevant site information; receive timely and accurate threat information and a mission objective(s) from a site; and then plan and rehearse a mission(s) prior to site entry.

- Licensees should identify a credible Mission Preparedness Time using data from real-world incidents or the drills or exercises at a site.

- Prior to a site being built and beginning operation, exercise data will likely not be available; under such circumstances, licensees should base Mission Preparedness Time estimates from discussions or tabletop exercises with law enforcement or other offsite armed response personnel, or on planning time data obtained from law enforcement or other offsite armed response personnel for similar emergencies at comparable facilities (i.e., complex industrial environments and secure facilities).

3.3.2 It is unlikely that law enforcement or other offsite armed response personnel will initially be familiar or have experience with an DBT adversary with the attributes, characteristics, and capabilities described in 10 CFR 73.1(a) and Revision 1 to Regulatory Guide (RG) 5.69.

- Licensees should ensure that law enforcement or other offsite armed response personnel fully know and understand the DBT of radiological sabotage and are able to prepare to successfully interdict and neutralize threats up to and including it.

- When identifying Mission Preparedness Time based on discussions, tabletop exercises, or planning time data from similar emergencies at comparable facilities, licensees and law enforcement or other offsite armed response personnel should determine whether additional time should be added to account for the DBT adversary's capability to potentially delay or disrupt response operations to a greater degree than law enforcement or other offsite armed responders may typically encounter.

3.3.3 To the extent practical, licensees should replicate real-world conditions during drills and exercises.

- Licensees should use only the personnel, locations, and equipment that would actually be involved with the emergency response.

- Licensees may use role players during drills or exercises in lieu of on-shift personnel; role players should possess the same knowledge, skills, and abilities as their on-shift counterparts.

- To the extent practical, licensees should ensure that role players and other drill and exercise participants use real-world equipment and locations when such use does not present an unacceptable risk to personnel or plant safety.

- For example, if a licensee uses a role player to simulate a control room operator, the role player should be stationed inside the actual control room and use the control room's communications and other equipment if the licensee can continue to safety operate the plant during the exercise.

- When it is not practical to use real-world equipment or locations, licensees should ensure that artificialities replicate real-world conditions to the maximum extent possible (e.g., control room simulators), so that they do not result in inaccurate assumptions, outcomes, or training, including negative training for drill and exercise participants.

3.3.4 There is an inverse relationship between a licensee's level of effort to inform and train law enforcement or other offsite armed response personnel and the amount of time those responders will need for planning purposes.

- That relationship should incentivize licensees to offer sufficient and quality information and frequent and quality training to law enforcement or other offsite armed response personnel to enable them to plan missions in the least amount of time possible.

- Licensees may discover that if the information and training they provide is effective, law enforcement or other offsite armed response personnel may become familiar enough with a site, the DBT adversary, and mission objectives that rehearsal and planning time is not needed, and offsite armed responders can go directly to a site and begin their mission(s).

- The benefit of establishing this level of proficiency is that Mission Preparedness Time becomes zero (or near zero), which results in a shorter AIPT.

3.3.5 Licensees that want opportunities to periodically establish shorter Mission Preparedness Times and use those times to recalculate their AIPTs should use mission preparedness data from the most recent 3-year period. Using data from the past 3 years should:

- result in AIPTs that more accurately reflect licensees' and LE or other offsite armed responders' current performance capabilities, and

- provide the flexibility for licensees to credit shorter Mission Preparedness Times (and by extension shorter AIPTs) as their and law enforcement or other offsite armed responders' knowledge, training, and performance improves.

Licensees should document mission planning times from all real-world incidents and drills and exercises at their facilities.

Licensees should also ensure that the data used to calculate AIPTs represent law enforcement or other offsite armed responders' mission preparedness times for a wide range of DBT scenarios; licensees should not rely on mission preparedness data that, collectively, exclude threats from either end of that spectrum.

3.3.6 A licensee with fewer than 3 years of data should use the longest documented Mission Preparedness Time in its AIPT calculations.

After a licensee has documented mission preparedness times for at least 3 years from real-world incidents, drills, or exercises, and for a variety of DBT scenarios, the licensee may use a Mission Preparedness Time that represents the 75th percentile in its AIPT calculation.

To calculate the 75th percentile, a licensee should use one of these two methods:

3.3.6.1 Method 1 - Calculate the 75th percentile electronically using a spreadsheet application:

3.3.6.1.1 Place individual data points (i.e., the mission preparedness times from real-world incidents and drills and exercises over the last 3 years) into separate, contiguous cells in a spreadsheet.

3.3.6.1.2 Use the percentile function to calculate the 75th percentile.

3.3.6.1.3 For example, consider a data set with the following 10 mission preparedness times: 147, 118, 82, 90, 102, 111, 89, 126, 141, and 74 minutes.

3.3.6.1.4 A licensee would enter each of the 10 mission preparedness times into separate cells within a contiguous range in a spreadsheet. For this example, assume the licensee entered the times into cells B9 through B18, inclusive.

3.3.6.1.5 In a blank cell on the same spreadsheet as the data range, a licensee would use the *PERCENTILE.INC (array, k)* formula, where "array" represents the range of data cells and "k" represents the percentile in decimal form. In this example, a licensee would enter the following formula into a blank cell to identify the 75th percentile for the sample data set: =PERCENTILE.INC (B9:B18, 0.75).

3.3.6.1.6 The spreadsheet application should produce the result of 124. Because 124 minutes represents the 75th percentile, a licensee would use 124 minutes as the Mission Preparedness Time for its AIPT calculation.

3.3.6.2 Method 2 - Calculate the 75th percentile manually by performing the following steps:

3.3.6.2.1 Order individual data points (i.e., the mission preparedness times
from real-world incidents and drills and exercises overt the last 3 years) from the shortest to longest times.

3.3.6.2.2 Multiply the total number of data points, N, by 75 percent (i.e., 0.75). If a licensee has 12 data points, N would equal 12.

3.3.6.2.3 Multiplying N by a percent produces a number that is called an index. For example, 12 x 0.75 equals 9, so the index would be 9.

3.3.6.2.4 If the index is a whole number, count the values in the data set from left to right (i.e., from the shortest to the longest time) until the index number of data points is reached.

3.3.6.2.4.1 The 75^{th} percentile is the average of that corresponding value in the data set and the value that directly follows it.

3.3.6.2.5 For example, consider a data set with the following 12 mission preparedness times: 60, 60, 72, 85, 93, 106, 110, 113, 120, 124, 130, and 145 minutes.

3.3.6.2.6 Using a whole number index of 9, the 75^{th} percentile would be represented by the average of 120 minutes (i.e., the ninth position in the data set) and 124 minutes (i.e., the tenth position in the data set).

3.3.6.2.6.1 Therefore the 75^{th} percentile would be (120 + 124) / 2 = 244/2 = 122 minutes.

3.3.6.2.6.2 A licensee would use 122 minutes as the Mission Preparedness Time for its AIPT calculation.

3.3.6.2.7 If the index is not a whole number, round it up to the nearest whole number.

3.3.6.2.8 Then, count the values in the data set from left to right (i.e., from the shortest to the longest time) until the index number of data points is reached.

3.3.6.2.9 The corresponding time represented by the index data point is the 75^{th} percentile.

3.3.6.2.10 For example, consider a data set with the following 13 mission preparedness times: 60, 60, 72, 85, 93, 106, 110, 113, 120, 124, 130, 135, and 145 minutes.

3.3.6.2.11 The index number for this data set would be 13 times 0.75, which equals 9.75. Since 9.75 is not a whole number, round the index up to a whole number, which in this example would be from 9.75 to 10.

3.3.6.2.12 The time in the tenth position in the sample data set is 124 minutes.

3.3.6.2.13 Because 124 minutes represents the 75th percentile in this data set, a licensee would use 124 minutes as the Mission Preparedness Time for its calculation.

3.4 Mission Execution Time

3.4.1 Mission Execution Time represents the period from when offsite armed responders depart the mission planning and rehearsal location (e.g., staging area) or arrive onsite and begin their missions (if the responders traveled directly to the site) and continues until all known adversaries are neutralized (i.e., for an adversary-focused-mission) or site staff completes preventative or mitigative actions to maintain the site at, or return the site to, a safe condition (i.e., for a plant condition-focused mission).

- Licensees should identify a credible Mission Execution Time using data from real-world incidents at a site or the annual drills or exercises.

3.4.2 Prior to a site being built and beginning operation, exercise data will likely not be available; under such circumstances, licensees should base Mission Execution Time estimates on discussions or tabletop exercises with law enforcement or other offsite armed response personnel, or on execution time data obtained from law enforcement or other offsite armed response personnel for similar emergencies at comparable facilities (i.e., complex industrial environments and secure facilities).

3.4.3 Licensees that use information or results from security modeling or vulnerability assessment software applications to inform their Mission Execution Time estimates should employ only software applications that are accredited by a U.S. government agency for the function(s) being analyzed (e.g., pathway analysis, combat simulation, system effectiveness).

- Additionally, licensees should ensure that any data used in such software applications accurately represent the actual capabilities, performance, training, and other related characteristics of the law enforcement or other offsite armed responders (i.e., not a default or unrelated defensive force), as well as the full capabilities of the DBT adversary (i.e., not exercise-related limitations associated with the site or the NRC's mock adversary force).

3.4.4 Licensees should ensure that law enforcement or other offsite armed response personnel fully know and understand the DBT of radiological sabotage and possess the knowledge, skills, abilities, and equipment to successfully interdict and neutralize threats up to and including it.

- When identifying Mission Execution Time based on discussions, tabletop exercises, or execution time data from similar emergencies at comparable facilities, licensees and LE or other offsite armed response personnel should determine whether additional time should be added to account for the DBT adversary's capability to potentially delay or disrupt response operations to a

greater degree than law enforcement or other offsite armed responders may typically encounter.

3.4.5 For plant condition-focused missions, Mission Execution Time should include the credible task time for preventative or mitigative actions that a licensee may need to take.

To identify a credible preventative or mitigative action task time, licensees should refer to performance testing or training times for an action, or site procedures such as abnormal or emergency operating conditions, diverse and flexible coping strategies, severe accident management guidelines, extensive damage mitigation guidelines, or other relevant documentation.

Licensees should be mindful that preventative or mitigative actions for plant condition-focused missions would be occurring within an actively hostile environment (i.e., known adversaries would not be neutralized before commencing preventative or mitigative actions); therefore, licensees should determine how much additional time needs to be added to the normal task times to account for delays that may be caused by an adversary, security force engagement of an adversary, or implementing localized security measures immediately prior to, or simultaneous with, the preventative or mitigative actions.

For example, licensee personnel would likely not be able to reach or move equipment stored outside a main protected area until armed response personnel are in position to facilitate movement of personnel or equipment.

In addition to the normal task time related to the deployment of that equipment, a licensee would have to consider how armed response personnel would facilitate that action and include the additional time in its Mission Execution Time estimate.

The need to add additional time may be caused by numerous factors, including:

- offsite armed responders navigating to onsite personnel, escorting them to equipment stored in an owner-controlled area (OCA), and then reentering the site together with the equipment;

- offsite armed personnel rendezvousing with recalled offsite licensee personnel and entering the site together with the equipment;

- offsite armed responders navigating to high ground like the rooftops of protected area buildings so armed responders can use their weapons to cover fire hose or power cable runs in outdoor areas without positioning themselves in the target area; or

- armed response personnel sweeping, clearing, and securing interior passageways and locations for planned preventative or mitigative actions.

3.4.6 There is an inverse relationship between a licensee's level of effort to inform and train LE or other offsite armed response personnel and the amount of time those responders will need for planning purposes.

- That relationship should incentivize licensees to offer sufficient and quality information and frequent and quality training to law enforcement or other offsite armed response personnel to enable them to plan missions in the least amount of time possible.

Licensees may discover that if the information and training they provide is effective, law enforcement or other response personnel may become familiar enough with a site, the DBT adversary, and mission objectives that Mission Execution Time may be reduced from hours to minutes.

The benefit of establishing this level of proficiency is Mission Execution Time is minimized, which results in a shorter AIPT.

3.4.7 Licensees that want opportunities to periodically establish shorter Mission Execution Times and use those times to recalculate their AIPTs should use mission execution data from the most recent 3-year period.

Using data from the past 3 years should

- Result in AIPTs that more accurately reflect licensees' and law enforcement or other offsite armed responders' current performance capabilities, and

- Provide the flexibility for licensees to credit shorter Mission Execution Times (and by extension shorter AIPTs) as their and law enforcement or other offsite armed responders' knowledge, training, and performance improves.

Licensees should document mission execution times from all real-world incidents and drills and exercises at their facilities.

Licensees should also ensure that the data used to calculate AIPTs represent law enforcement or other offsite armed responders' mission execution times for a wide range of DBT scenarios; licensees should not rely on mission execution data that, collectively, exclude threats from either end of that spectrum.

3.4.8 A licensee with fewer than 3 years of data should use the longest documented Mission Execution Time in its AIPT calculations.

After a licensee has documented mission execution times for at least 3 years from real-world incidents, drills, or exercises, and for a variety of DBT scenarios, the licensee may use a Mission Execution Time that represents the 75^{th} percentile in its AIPT calculation.

To calculate the 75^{th} percentile, a licensee should use one of the two methods described in Staff Regulatory Guidance Position 3.3.6 of this appendix.

3.5 Safety Margin Time

3.5.1 Safety margin time attempts to account for the uncertainties that may exist in the data used to calculate an AIPT, or different conditions at the time of an attack than those considered or assumed by a licensee's AIPT calculation methodology.

Examples of uncertainties include:

- Potential inclement weather;
- Chemical (including reactor coolants and moderators), industrial (e.g., steam, flooding/drowning, confined space), environmental (e.g., heat), or radiological hazards;
- Traffic conditions;
- Communications challenges;
- Competing demands for offsite responder resources; unanticipated decisions or actions by offsite armed responders (e.g., implementing isolate-and-contain protocols rather than those for active shooters);
- Estimating times using response data or assumptions involving threats with lesser capabilities than the DBT of radiological sabotage;
- Damage or destruction of more than the equipment in a single target set by an adversary;
- Inadvertent destruction of target set or other plant equipment by less than fully trained or knowledgeable armed response personnel;
- An adversary's use of unexpected or more effective tactics; inoperable mitigation equipment;
- Obstructed pathways on or near the site; and
- Uncertainties associated with the use of exercise data, where times may be more favorable because the activities were planned and announced.

3.5.2 A licensee should use a safety margin of 25% of the total of AIPT time elements 2 through 4 (i.e., Response Time, Mission Preparedness Time, Mission Execution Time) for its AIPT calculation.

4. EXAMPLES

4.1 Example 1

Licensee facility in an urban area

Bounding mission: Adversary-focused

Calculation:

Alarm Assessment and Communication Time 16 minutes
1 minute to receive and assess alarm
15 minutes to notify offsite armed responders

Response Time 1½ hours
city police tactical team(s) establishes a near-site staging area

Mission Preparedness Time 4 hours
lack of familiarity with facility, adversary, and potential missions

Mission Execution Time 2½ hours
travel to the site, negotiate delay features, neutralize adversary

Subtotal: 8 hours, 16 minutes

Safety Margin Time (25% of elements 2 through 4)
1½ + 4 + 2½ = 8 x .25 = 2 hours + 2 hours, 0 minutes
10 hours, 16 minutes

(round to the next ½ hour increment) AIPT = 10½ hours

4.2 Example 2

Licensee facility in a rural location

Bounding mission: Plant condition-focused

Calculation:

Alarm Assessment and Communication Time 20 minutes
5 minutes to receive and assess alarm
15 minutes to notify offsite armed responders

Response Time 4 hours
regional tactical team responds directly to the site
small elements enter site upon arrival, rather than wait outside to assemble a full team

Mission Preparedness Time 0 minutes
responders very familiar with the facility and design basis threat, so they complete preparations while responding

Mission Execution Time 3 hours
able to quickly negotiate delay features, neutralize adversary in safety-related plant areas, and protect site personnel during preventative actions

Subtotal: 7 hours, 20 minutes

Safety Margin Time (25% of AIPT elements 2 thru 4)
4 + 0 + 3 = 7 x .25 = 1¾ hours + 1 hour, 45 minutes
9 hours, 5 minutes

(round to the next ½ hour increment) AIPT = 9½ hours

APPENDIX D
REACTOR FACILITY INFORMATION THAT LICENSEES SHOULD PROVIDE TO LAW ENFORCEMENT OR OTHER OFFSITE ARMED RESPONDERS

In accordance with the requirement in 10 CFR 2.390(d)(1) and Section 312.2 in Volume 1 of Revision 1 to DG-SGI-1, "Designation Guide for Safeguards Information," dated February 26, 2025 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML24156A074), the items, actions, and rationales in Appendix D of this document has been designated as, "Official Use Only – Security-Related Information (OUO-SRI)." Therefore, Appendix D has been removed from this document and has been identified and issued separately as Regulatory Guide 5.97.1.

Appendix D of this document is not publicly available at this time.

If you are an NRC applicant, licensee, or certificate holder and want to review this document, please contact your company's licensing manager, onsite NRC inspector, or NRC Project Manager to request a copy.

If you are not an NRC applicant, licensee, or certificate holder, and wish to obtain a copy of this document, please send a request to FOIA.Resource@nrc.gov, in accordance with NRC Management Directive 3.1, "Freedom of Information Act."

BIBLIOGRAPHY

1. U.S. Nuclear Regulatory Commission (NRC), Regulatory Issue Summary (RIS) 2002-12A: "NRC Threat Advisory and Protective Measures System."
2. NRC, RIS 2002-21, "National Guard and Other Emergency Responders Located in the Licensee's Controlled Area."
3. NRC, RIS 2006-02, "Good Practices for Licensee Performance During the Emergency Preparedness Component of Force-On-Force Exercises."
4. NRC, RIS 2007-02, "Clarification of NRC Guidance for Emergency Notifications During Quickly Changing Events."
5. NRC, Information Notice (IN) 2007-12, "Tactical Communications Interoperability Between Nuclear Power Reactor Licensees and First Responders."
6. Nuclear Energy Institute (NEI) White Paper – "Best Practices for Maintaining Relationships with Law Enforcement Agencies and First Responders at Nuclear Reactor Facilities," February 2010.
7. NEI 12-03, "Security Operating Experience Submittal Guideline."
8. U.S. Department of Energy, Sandia National Laboratories, SAND99-2486, "Explosive Protection."
9. U.S. Department of Defense, "Structures to Resist the Effects of Accidental Explosions," United Facilities Criteria (UFC) 3-340-02.