U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-5072

Proposed new Regulatory Guide 5.90

Issue Date: July 2024
Technical Lead: Beth Reed

Guidance for Alternative Physical Security Requirements for Small Modular Reactors and Non-Light-Water Reactors

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes methods and approaches the staff of the U.S. Nuclear Regulatory Commission (NRC) consider acceptable for use by licensees of small modular reactors (SMRs), as defined in Title 10 of the *Code of Federal Regulations* (10 CFR) 171.5, "Definitions" (Ref. 1), and non-light-water reactors (non-LWRs) to comply with requirements in 10 CFR 73.55(s), "Alternative physical security requirements" (Ref. 2)

This RG provides an acceptable method that applicants and licensees may use in determining if they are eligible to use one or more of the alternative physical security requirements in 10 CFR 73.55(s). It also provides guidance on implementation of these requirements. This guidance should assist applicants in the design of a physical protection program that meets NRC regulatory requirements. This guidance is not intended to be all-inclusive. Licensees and applicants may employ alternative methods, after receiving NRC approval, that satisfy compliance with the requirements in 10 CFR Part 73 (Ref. 3). Each licensee should account for and determine the measures needed for compliance with the applicable requirements in

- 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 4),
- 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 5),
- 10 CFR Part 73, "Physical Protection of Plants and Materials."

The licensee bears sole responsibility for developing a physical protection program that will ensure that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

Applicability

This RG is for use by applicants and holders of an operating license (OL) or a combined license (COL) for SMRs, as defined in 10 CFR 171.5 and non-LWRs licensed under the provisions of 10 CFR Part 50 or 10 CFR Part 52 to satisfy the requirements of 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage." Use of this RG will assist such applicants and licensees in developing and maintaining, or alternatively submitting to the NRC when required, complete and accurate information that sufficiently describes the alternative physical security requirements being implemented and the technical basis supporting the use of such requirements. These alternative physical security requirements should be documented in the facility's physical security plan (PSP) submitted to the NRC for review and approval. The technical analysis supporting the use of an

alternative physical security requirement need not be submitted to the NRC but must be maintained and is subject to inspection.

Applicable Regulations

- 10 CFR Part 50 provides regulations for licensing production and utilization facilities.
    - 50.34, "Contents of applications; technical information," requires applications for a construction permit to have a preliminary and a final safety analysis report.
        - 10 CFR 50.34(c), "Physical Security Plan", requires an applicant for an OL for a production or utilization facility that will be subject to the requirements of 10 CFR 73.50 to have a physical security plan, a training and qualification plan that meets the criteria in Appendix B "General Criteria for Security Personnel," to 10 CFR Part 73, and a cyber security plan that complies with the criteria in 10 CFR 73.54.
        - 10 CFR 50.34(d)(2) requires an applicant for an OL for a utilization facility that will be subject to the requirements of 10 CFR 73.55 to have a safeguards contingency plan (SCP) that meets the criteria in 10 CFR Part 73, Appendix C, "Licensee Safeguards Contingency Plans."
    - 10 CFR 50.54(p)(5) requires a licensee that makes changes to its facility to consider the effect of the changes on its site-specific analysis prepared under 10 CFR 73.55(s)(1)(iv).
- 10 CFR Part 52 governs the issuance of early site permits, standard design certifications, combined licenses, standard design approvals, and manufacturing licenses for nuclear power facilities.
    - 10 CFR 52.79, "Contents of applications; technical information in final safety analysis report," requires an applicant to provide a final safety analysis report describing the facility, design bases, limits or operation, and its structures, systems, and components (SSCs) of the facility as a whole. Specifically,
        - 10 CFR 52.79(a)(35)(i) requires an applicant to submit a PSP.
        - 10 CFR 52.79(a)(35)(ii) requires an applicant to submit a description of the implementation of the PSP .
        - 10 CFR 52.79(a)(36)(i) requires an applicant to submit a SCP.
- 10 CFR Part 73 provides the requirements for the establishment and maintenance of a physical protection system that will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used.
    - 10 CFR 73.50, "Requirements for physical protection of licensed activities," requires licensees to establish a security organization, physical barriers, access requirements, detection aids, communications, testing, maintenance, and SCP.
    - 10 CFR 73.55 requires licensees to establish and maintain physical protection programs to provide high assurance that activities involving special nuclear material are not

inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

- 10 CFR 73, Appendix B, Section VI.A.1 requires licensees to ensure that all individuals who are assigned duties and responsibilities required to prevent significant core damage and spent fuel sabotage, implement the Commission-approved security plans, licensee response strategy, and implementing procedures, meet minimum training and qualification requirements to ensure individuals possess the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities.

Related Guidance

Applicants or licensees may consider the following related guidance when using this RG. The list of related guidance may assist applicants or licensees in the implementation of an elected alternative physical security requirement found in 10 CFR 75.55(s)(2). It may also assist in the preparation of design and licensing basis information to support an application to the NRC. Some of the related guidance documents referenced below are written mainly for light-water nuclear power reactors (LLWRs). These documents were developed to provide guidance for LLWRs and focus on protecting against the design basis threat (DBT) or radiological sabotage by preventing significant core damage and spent fuel sabotage. However, applicants or licensees may find the information, methods or approaches described in these related guidance documents to be useful in their design of physical security engineered and administrative controls and management systems for implementing alternative requirements. They may also be useful in developing methods or approaches for analyzing security-initiated events, characterizing source terms, and determining radiological consequences of those events. The staff may use the guidance as applicable in the review of the applicants' or licensees' approaches for the design of the facility and the physical protection system.

- RG 1.145, "Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants," (Ref. 6) provides criteria for characterizing atmospheric dispersion conditions for evaluating the consequences of accidental radiological releases to the exclusion area boundary and outer boundary of the low population zone for nuclear power plants.

- RG 1.183, "Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors," (Ref. 7) provides guidance on design basis accident radiological consequence analyses for light-water nuclear power reactors, including the development of design basis accident radiological source terms used in siting and safety analyses.

- RG 1.194, "Atmospheric Relative Concentrations for Control Room Radiological Habitability Assessments at Nuclear Power Plants," (Ref. 8) provides guidance on determining atmospheric relative concentration (χ/Q) values in support of design basis control room radiological habitability assessments at nuclear power plants.

- RG 1.233, "Guidance for a Technology-Inclusive, Rick-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," (Ref. 9) provides guidance on using a technology-inclusive, risk-informed, and performance-based methodology to inform the licensing basis and content of applications for non-light-water reactors (non-LWRs), including, but not limited to, molten salt reactors, high-temperature gas-cooled reactors, and a variety of fast reactors at different thermal capacities. This RG may be used by non-LWR applicants applying for permits, licenses, certifications, and approvals under 10 CFR Part 50, "Domestic Licensing of

Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

- RG 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Protection Program that Meets 10 CFR 73.55 Requirements," (SGI) (Ref. 10) describes the safeguards details for the DBT of radiological sabotage, including the attributes, characteristics, and capabilities of the DBT adversary. These attributes, characteristics, and capabilities assist a licensee in the design, development, and implementation of a physical security system and associated programs.

- RG 5.71, "Cyber Security Programs for Nuclear Facilities," (Ref. 11) provides an approach that the NRC staff considers acceptable for complying with the NRC regulations for the protection of digital computers, communications systems, and networks from a cyber-attack, to include that associated with the DBT of radiological sabotage.

- RG 5.74, "Managing the Safety/Security Interface," (Ref. 12) provides a method of compliance for managing the interface between safety and security.

- RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities," (Ref. 13) provides an approach that the NRC staff considers acceptable for complying with the NRC regulations for the 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. 14) provides approaches on meeting the requirements of 10 CFR 73.55 for licensee design and implementation of a physical protection program.

- RG 5.77, "Insider Mitigation Program," (SGI) (Ref. 15) describes an acceptable approach for an insider mitigation program for protecting nuclear power reactors against malicious acts.

- RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors," (Official Use Only (OUO), not publicly available) (Ref. 16) describes approaches and methodologies that the NRC considers acceptable for meeting the requirements of 10 CFR 73.55.

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

    - 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; the administrative controls; and management systems for operations and organization.

    - Section 13.6.2, "Physical Security - Review of Physical Security System Designs - Standard Design Certification and Operating Reactor Licensing Applications," provides guidance for the physical security review of designs of physical security systems.

- NUREG/CR-7145, "Nuclear Power Plant Security Assessment Guide," (Ref. 18) describes an acceptable approach for performing security assessment 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," (Ref. 19) provides technical details applicable on 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," (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 design to protect against the explosives.

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

- U.S. Department of Energy, Sandia National Laboratory, SAND99-2168, "Access Delay Technology," (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.

- U.S. Department of Energy, Sandia National Laboratory, SAND2008-5644, "Vital Area Identification for U.S. Regulatory Nuclear Power Reactor Licensees and New Reactor Applicants," (Ref. 23) describes a systematic process involving logic models for the identification of the minimum set of areas that must be designated as vital areas in order to ensure that all radiological sabotage scenarios are prevented.

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

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses. RGs 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 50, 10 CFR Part 52, 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), approval numbers 3150-0011, 3150-0151, and 3150-0002. 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 e-mail to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202 (3150-0011, 3150-0015 and 3150-0002) Office of Management and Budget, 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.

B. DISCUSSION

Reason for Issuance

This new guidance addresses the requirements for an applicant for, or holder of a license for an SMR, as defined in 10 CFR 171.5, or non-LWR licensed under the provisions of 10 CFR Part 50 or 10 CFR Part 52 to apply select alternatives to requirements in 10 CFR 73.55 for physical security of advanced reactors, which, for purposes of this RG, are SMRs and non-LWRs.

Background

The current fleet of operating reactors are Generation III LWRs. It is likely that the NRC will receive applications to license advanced reactors, either non-LWRs or SMRs under 10 CFR Part 50 or 10 CFR Part 52. Before approving these applications and issuing a license, the NRC must make the following findings:

- The applicable standards and requirements of the Atomic Energy Act of 1954, as amended (also referred to as the Act) (Ref. 25), and the NRC's regulations are met.

- The facility will operate in conformity with the license as amended, the provisions of the Act, and the NRC's regulations.

- There is reasonable assurance that
  (i) the activities authorized by the OL can be conducted without endangering the health and safety of the public, and
  (ii) such activities will be conducted in compliance with the regulations of 10 CFR Part 50 or 10 CFR Part 52.

- Issuance of the license is not inimical to the common defense and security or to the health and safety of the public.

Advanced reactors licensed under 10 CFR Part 50 or 10 CFR Part 52 would be subject to the regulatory framework and security requirements in 10 CFR 73.55. This regulatory framework provides high assurance[1] that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. Consistent with this regulatory framework, licensees must develop, implement, and maintain a physical protection program that protects against the DBT of radiological sabotage. This physical protection program is implemented through a licensee's PSP which details how the licensee will meet the performance objective and implement the security requirements in § 73.55.

Typically, a Part 50 or Part 52 license contains a license condition requiring the licensee to operate in accordance with its NRC approved security plans. Accordingly, an applicant's or licensee's PSP contains information that becomes a part of the licensing basis for the facility (required by 10 CFR 50.34(c)(1)-(3), 10 CFR 50.34(d), 10 CFR 50.34(e), 10 CFR 52.79(a)(35)(i), 10 CFR 52.79(a)(36)(i), and 10 CFR

---

[1] The Commission stated in staff requirements memorandum (SRM) "SRM-SECY-16-0073 – Options and Recommendations for the Force-On-Force Inspection Program in Response to SRM-SECY-14-0088," dated October 5, 2016, that "the concept of 'high assurance' of adequate protection found in the NRC security regulations is equivalent to 'reasonable assurance' when it comes to determining what level of regulation is appropriate." The Commission re-iterated this point in "SRM-SECY-18-0076 – Options and Recommendation for Physical Security for Advanced Reactors," dated November 19, 2018.

52.79(a)(36)(ii)). The PSP must be maintained until the certifications required by 10 CFR 50.82(a)(1) or 10 CFR 52.110(a) have been submitted by the licensee.

Many future advanced reactor designs may rely on passive safety features to perform safety functions without any human action. Based on inherent design features, including these passive safety features and small reactor sizes, some applicants for OLs or COLs under 10 CFR Part 50 or 10 CFR Part 52 may seek alternative physical security requirements rather than implementing certain existing security requirements in 10 CFR 73.55. These alternative physical security requirements would be documented in the applicant's or licensee's PSP's and become a part of the licensing basis of the facility.

The NRC will approve PSPs if they contain sufficient detail to enable the NRC to determine that the applicant or licensee will meet all applicable requirements in 10 CFR 73.55 and therefore be able to protect against the DBT of radiological sabotage. The NRC staff uses the Standard Review Plan (SRP), Section 13.6.1, "Physical Security - Combined License and Operating Reactors," as guidance during its review of license application, including the applicant's security plans, and any security plan amendments submitted for NRC review and approval. The SRP is not a substitute for the NRC's regulations, and compliance with it is not required. However, the SRP provides guidance that may be useful to an applicant or licensee in its preparation of the security plan or security plan amendments to ensure that they contain the detailed information necessary to demonstrate how regulatory requirements (e.g., selected alternative security requirements) will be met.

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).

Pertinent to this RG, the following IAEA documents were considered in the development of this RG:

- IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)" (Ref. 28), issued January 2011, contains recommended operational guidance for the protection of nuclear facilities from the threat of radiological sabotage, along with training and operational readiness of security personnel.

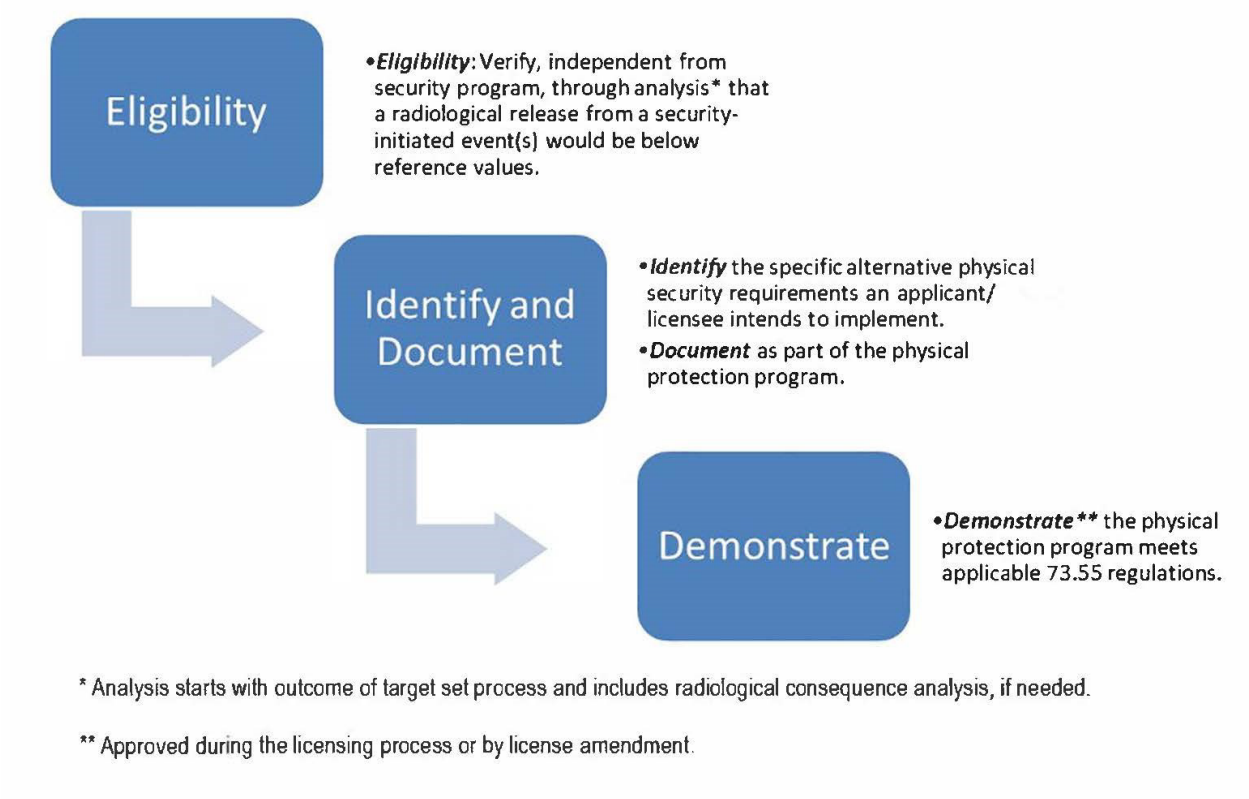
- IAEA Nuclear Security Series No. 27-G, "Physical Protection of Nuclear Material and Nuclear Facilities (implementation of INFCIRC/225/Revision 5)" (Ref. 29), issued April 2018, contains guidance on implementing recommendations found in INFCIRC/225/Revision 5 in establishing, strengthening, and sustaining physical protection systems.

C. STAFF REGULATORY GUIDANCE

This section describes the process an applicant or licensee of an SMR, as defined in 10 CFR 171.5, or a non-LWR, that is licensed under the provisions of 10 CFR Part 50 or 10 CFR Part 52, should use to determine eligibility and the capability to implement the alternative requirements identified in 10 CFR 73.55(s)(2).

Figure 1 provides a high-level flow chart of the process for determining an applicant's or licensee's eligibility to use the alternative security requirements and document compliance with the performance objective in 10 CFR 73.55(b), with the alternatives applied.

Figure 1



1. Conditions for applying selected alternatives in accordance with 10 CFR 73.55(s)(1)(i), "Applicability"

10 CFR 73.55(s)(1)(i) allows an applicant or licensee of an SMR or non-LWR licensed under the provisions of 10 CFR Part 50 or 10 CFR Part 52 to elect to use one or more of the alternatives to certain security requirements as specified in 10 CFR 73.55(s)(2), if the applicant or licensee determines it is eligible as specified in 10 CFR 73.55(s)(1)(ii).

1.1 An applicant or licensee that is **not** an SMR, as defined in 10 CFR 171.5, or non-LWR, that is licensed under the provisions of 10 CFR Part 50, or is **not** a holder of a COL for an SMR or non-LWR, under the provisions of 10 CFR Part 52:

1.1.1 may **not** elect to use one or more of the alternatives to certain security requirements as specified in 10 CFR 73.55(s)(2).

1.1.2 may request authorization to meet one or more of the alternatives described in 10 CFR 73.55(s)(2) by submitting an application to the NRC under the provisions of 10 CFR 73.55(r), "Alternative measures." When necessary, applications should also request an exemption(s) from specific requirements of 10 CFR 73.55 under the provision of 10 CFR 73.5, "Specific exemptions."

2. Eligibility to use selected alternatives in accordance with the 10 CFR 73.55(s)(1)(ii), "Eligibility"

The requirements in 10 CFR 73.55(s)(1)(ii) state that an applicant or licensee that elects to use one or more of the alternatives in 10 CFR 73.55(s)(2) must "demonstrate that the consequences of a postulated radiological release that could result from a postulated security-initiated event do not exceed the offsite dose reference values defined in 10 CFR 50.34(a)(1)(D) and 10 CFR 52.79(a)(1)(vi) …."

2.1 To demonstrate eligibility, an applicant or licensee may rely on information from the safety analysis and the target set identification process to inform the radiological dose consequence determination.

2.2 While the safety analysis information is based on accident scenarios, security-initiated events could have similar results. The licensee or applicant would have to verify a security event would not cause the formation of additional release pathways or cause a higher release fraction than a safety event may release.

3. **Identifying and documenting selected alternatives in accordance with 10 CFR 73.55(s)(1)(iii), "Identification and documentation"**

The requirements in 10 CFR 73.55(s)(1)(iii) state that an applicant or licensee that elects to use one or more of the alternatives in 10 CFR 73.55(s)(2) must "identify the specific alternative physical security requirement(s) it intends to implement as part of its physical protection program and demonstrate how the requirements set forth in 10 CFR 73.55 are met when the selected alternative(s) is used."

3.1 A licensee or applicant electing to implement one or more of the alternatives found in 10 CFR 73.55(s)(2) should describe the following in its security plans (i.e. PSP, Training and Qualification Plan (TQ&P), SCP, or Cyber Security Plan (CSP), as applicable):

3.1.1 how it intends to implement the alternative physical security requirement(s), and

3.1.2 how the general performance objective and requirements in 73.55(b) are met.

3.2 The descriptions in the security plans mentioned in section 3.1 should be sufficiently detailed to allow the NRC to determine a that the alternative physical security requirement, combined with all other requirements, provides reasonable assurance that the DBT of radiological sabotage can be defeated.

3.2.1 For example, if an applicant or licensee elected to implement the alternative offsite secondary alarm station (SAS) requirement in 10 CFR 73.55(s)(2)(iv), it would have to describe in its security plans how the offsite SAS would meet the requirements in 10 CFR 73.55(i), such as how it will ensure that intrusion detection system alarms and assessment

videos will annunciate and display concurrently in the central alarm station and the offsite SAS (as required by 10 CFR 73.55(i)(2)), and how it would meet the requirements in 10 CFR 73.55(i)(4) and other requirements in 10 CFR 73.55.

3.3 The full descriptions in these security plans must address how the alternative as applied, integrated with other requirements in 10 CFR 73.55 for design of a physical protection program and/or stand alone, meets the performance goal and requirements of 10 CFR 73.55(b).

3.3.1 For example, the PSP, in accordance with 10 CFR 73.55(c)(1), should describe how the licensee will implement the requirements in 10 CFR 73.55, which includes how the licensee will design and/or implement the selected alternative and use it to meet a required security function(s) and the performance objective and requirements of 10 CFR 73.55(b).

3.4 Applicants or licensees wishing to request additional alternatives not found in 10 CFR 73.55(s)(2) should use the exiting processes found in 10 CFR 73.5 and 10 CFR 73.55(r).

3.5 The physical protection program should be designed to protect against the DBT for radiological sabotage with the characteristics, capabilities and attributes described in 10 CFR 73.1, "Purpose and scope." In accordance with 10 CFR 73.1, the licensees must design their physical protection systems to protect against**:**

- violent external assaults and methods (10 CFR 73.1(a)(1)),
- assailants who are well-trained and dedicated, willing to kill or be killed, knowledgeable, active, and equipped (10 CFR 73.1(a)(1)(i)(A) through 10 CFR 73.1(a)(1)(i)(E)),
- internal threats (10 CFR 73.1(a)(1)(ii)),
- land vehicle bomb assaults (10 CFR 73.1(a)(1)(iii)),
- waterborne vehicle bomb assaults (10 CFR 73.1(a)(1)(iv)), and
- cyber-attacks (10 CFR 73.1(a)(1)(v)).

3.6 Licensees should refer to RG 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Protection Program that Meets 10 CFR 73.55 Requirements" (SGI), for detailed information regarding the Commission-determined characteristics, attributes, and capabilities of the DBT adversary that licensees must design their physical protection programs to protect against to prevent radiological sabotage as required by 10 CFR 73.55(b)(2).

4 Demonstrating Eligibility in accordance with 10 CFR 73.55(s)(1)(iv), "Analysis"

10 CFR 73.55(s)(1)(iv) requires that an applicant or licensee that elects to use one or more of the alternatives in 10 CFR 73.55(s)(2) must perform a technical analysis demonstrating how it meets the criteria in 10 CFR 73.55(s)(1)(ii).

4.1 This analysis must be maintained until the certifications required by 10 CFR 50.82(a)(1) or 10 CFR 52.110(a) have been submitted by the licensee.

4.2 If applicable, a licensee or applicant may utilize the analysis described in RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors" (Official Use Only (OUO), not publicly available), to determine eligibility. This analysis provides a more flexible approach with different criteria to determine eligibility.

4.2.1 If the SMR or non-LWR licensee or applicant does not have any achievable target sets at the end of the target set evaluation, then it is eligible to elect to use some or all of the alternative security measures found in 10 CFR 73.55(s)(2).

4.2.2 If a licensee or applicant does have achievable target sets at the end of the target set evaluation, then they could use an offsite radiological consequence analysis (hereafter referred to as a consequence analysis) to determine eligibility.

4.3 The consequence analysis should evaluate potential radiological releases from DBT-initiated or security-related events and ensure they are below 0.25 sievert (Sv) (25 rem) at the exclusion area boundary for the worst 2-hour period after the release and at the low population zone during the entire passage of the radioactive cloud and are within the site's security bounding time (SBT). See Appendix C for additional information regarding SBT, including how to calculate it.

4.4 For determining eligibility, a consequence analysis is an acceptable method to perform the analysis required by 10 CFR 73.55(s)(1)(iv).

4.4.1 A consequence analysis is performed by the applicant or licensee to determine potential radiation doses from exposure to the postulated radiological release plume at the exclusion area boundary for any two-hour period after initiation of the release and at the outer boundary of the low population zone for the duration of the passage of the plume.

4.4.2 The consequence analysis will evaluate DBT-initiated or security-related event scenarios based on achievable target sets.

4.5 A licensee or applicant wishing to demonstrate eligibility to use some or all of the alternative security measures found in 10 CFR 73.55(s)(2) should develop security-related scenarios that examine the capability to prevent or mitigate an offsite release from exceeding reference values defined in 10 CFR 50.34(a)(1)(ii)(D)(*1*) and (*2*) and 10 CFR 52.79(a)(1)(vi)(A) and (B). Some scenarios to evaluate could include, but are not limited to the following:

4.5.1 Some or all achievable target sets are compromised by an adversary, resulting in a release of radionuclides from any source in excess of the reference values defined in 10 CFR 50.34(a)(1)(ii)(D)(*1*) and (*2*) and 10 CFR 52.79(a)(1)(vi)(A) and (B).

4.5.2 Some or all achievable target sets can be compromised by an adversary, resulting in a release of radionuclides from any source, but the release can be mitigated before offsite doses exceed the reference values defined in 10 CFR 50.34(a)(1)(ii)(D)(*1*) and (*2*) and 10 CFR 52.79(a)(1)(vi)(A) and (B). Actions to mitigate a release can involve both onsite and offsite resources to interdict the adversary force and/or mitigate the release.

4.6 Licensees or applicants should discuss the inherent features, engineered features, or operator actions employed at the facility that would allow the radiological release to be delayed, minimized, or prevented for the evaluated security-related event scenarios, and the basis for the assumptions in the consequence analysis.

4.7 The consequence analysis should determine the type and amount of radioactivity potentially released to the environment and the potential for offsite consequences, if any. For each release scenario for which doses are assessed, a quantitative radiological source term should be developed by specifying atmospheric release characteristics such as the time dependent isotopic

release rates to the atmosphere, release durations, release locations, physical/chemical form (including particle size), and plume buoyancy.

4.7.1 The radiological source terms should be estimated for the specific facility using accepted analysis methods and codes, such as those used for the accident and radiological consequence analyses in the safety analysis report for the facility or in probabilistic risk assessment, justified for the conditions considered in the DBT-initiated or security-initiated event scenarios.

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

4.8.1 The analysis should also address potential changes to these physical properties from actions that could be taken by the DBT adversary during an attack (e.g., large explosions or fires, or incendiary devices) and how radionuclide transport may or may not be affected.

4.8.2 Physical and chemical processes affecting the timing, composition and magnitude of the release should be addressed, such as convective or conductive cooling, radioactive decay and in-growth corrections, and radionuclide removal or retention processes.

4.9 The analysis should describe any and all scenarios that could result in releases of radionuclides from any source. For the purposes of this analysis, a release from any source should not exceed the dose reference values defined in 10 CFR 50.34(a)(1)(ii)(D)(*1*) and (*2*) and 10 CFR 52.79(a)(1)(vi)(A) and (B).

4.10 The analysis should evaluate atmospheric release and direct dose contributors to doses at the exclusion area boundary and the outer boundary of the low population zone considering the site characteristics for the specific facility.

4.10.1 The atmospheric release may be modeled as a neutral density plume that does not undergo chemical or physical transformations after release to the atmosphere, with corrections for radioactive decay and in-growth, wet or dry deposition (or both), and plume rise due to buoyancy or momentum (or both), as appropriate.

4.10.2 If the chemical or physical form of the atmospheric release requires more complex atmospheric transport modeling due to varying fuel types, materials, and facility design or specifics of the evaluated event scenario, then additional analyses may be needed.

4.11 An atmospheric transport model appropriate for the range of distances under consideration should be identified.

4.11.1 The applicant or licensee should consider using a straight-line Gaussian plume segment-type atmospheric dispersion model to estimate short-term atmospheric concentrations, with modifications as needed to account for near field dispersion phenomena.

4.11.2 Acceptable atmospheric dispersion models for accidents as used in safety analyses are given in RG 1.145, “Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants,” and RG 1.194, “Atmospheric Relative Concentrations for Control Room Radiological Habitability Assessments at Nuclear

Power Plants." Such models are generally most suitable for relatively simple transport situations, such as open and level terrain, relatively steady meteorology, and relatively close distances (<10 kilometers). For models of these types, dispersion parameters appropriate to the characteristics of the area and distance ranges under consideration should be identified, and conceptual approaches for the treatment of wind shifts during the release and near field effects such as elevated releases, building wake effects, plume meander, and plume rise should also be identified.

4.11.3 Should an applicant or licensee determine that a Gaussian model is not ideal or practicable for the consequence analysis, they may choose to employ a different type of dispersion model with supporting technical basis.

4.11.4 Any assumptions made in the atmospheric transport model should be identified so that the analyst can evaluate the suitability of the model for their particular application.

4.12 Exposure parameters (e.g., shielding factors, breathing rates, exposure durations) should be characterized. The development of such parameters should not assume any credit for preplanned protective actions such as evacuation or sheltering.

4.13 Dose calculations should determine the total effective dose equivalent (TEDE), as defined in 10 CFR 50.2, "Definitions."

4.14 The dose estimation is carried out by combining the results of the release, transport, and potential exposure from a source term.

4.14.1 A recognized source of dose conversion factors should be used to estimate the TEDE to an individual at any point of the exclusion area boundary and any point on the outer boundary of the low population zone for comparison to the dose reference values defined in 10 CFR 50.34(a)(1)(ii)(D)(*1*) and (*2*) and 10 CFR 52.79(a)(1)(vi)(A) and (B).

4.14.2 Applicants may find guidance on offsite accident dose assessment considerations in RG 1.183, "Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors" to be helpful. Although the source term information in RG 1.183 is specific to LWR safety analysis, RG 1.183 provides useful information on calculation of offsite doses for accidents in general.

5 Alternative requirement for armed responders

In accordance with 10 CFR 73.55(s)(2)(i), a licensee that meets 10 CFR 73.55(s)(1) is relieved from the requirement for the minimum number of armed responders in 10 CFR 73.55(k)(5)(ii).

5.1 This alternative gives an advanced reactor licensee the flexibility to determine and use the number of onsite armed responders necessary to meet the requirements of 10 CFR 73.55(b)(3). Licensees may use existing methods, such as those employed by large, light-water reactor licensees, for determining the necessary number of onsite armed responders.

5.3 Under this proposal, a licensee would be permitted to design its physical protection program to potentially have fewer than ten onsite armed responders, including no onsite armed responders, if appropriate.

5.4 The number of onsite armed responders may be reduced to zero if the licensee also implements the alternative requirements in 10 CFR 73.55(s)(2)(ii) and relies on LE or other offsite armed responders to fulfill the interdiction and neutralization functions to protect against the DBT of

radiological sabotage. For a licensee that designs its physical protection system to rely on onsite armed responders to perform interdiction and neutralization to achieve the performance objective and requirements of 10 CFR 73.55(b), the physical security alternative provides relief only from the prescriptive requirement for the minimum number of armed responders; all other existing requirements associated with onsite armed personnel continue to apply.

6. Alternative requirements for interdiction and neutralization, relying on law enforcement (LE) or other offsite armed responders to fulfill the interdiction and neutralization capabilities

In accordance with 10 CFR 73.55(s)(2)(ii) and (s)(2)(ii)(A), *a licensee that meets 10 CFR 73.55(s)(1) and has no armed response personnel onsite whose primary duty is to respond to, interdict, and neutralize acts of radiological sabotage may rely on law enforcement or other offsite armed responders to fulfill the interdiction and neutralization functions required by 10 CFR 73.55(b)(3)(i).*

Section 10 CFR 73.55(b)(3)(i) requires that the licensee's 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. The alternative for relying on LE or other offsite armed responders to carry out the interdiction and neutralization capabilities is acceptable when the following are met by design of the licensee's physical protection system:

6.1 *Intrusion detection* - The capability to detect is met and maintained by the physical security SSCs relied on for interior and exterior intrusion detection functions and designed to provide reasonable assurance of detecting unauthorized access into vital and protected areas.

6.1.1 The licensee or applicant should design its intrusion detection systems to detect threats using the principle of diversity necessary for the reliability and availability of intended intrusion detection functions.

6.1.2 The licensee or applicant should utilize multiple, complementary intrusion detection systems to maximize the likelihood that at least one sensor system is operating during any environmental disturbance and minimize the possibility that an intruder will be able to use a single defeat method (e.g., running, walking, crawling, jumping, rolling, bridging, tunneling) to traverse a detection zone or portal without being detected.

6.2 *Intrusion assessment* - The capability to assess is met and maintained by the physical security SSCs relied on for intrusion assessment functions and designed to provide assurance of rapid remote assessment for determining cause and initiating appropriate security responses.

6.2.1 The licensee or applicant should apply to the design of a physical protection system the principle of diversity necessary for the reliability and availability of systems and components to achieve the intended intrusion assessment functions.

6.3 *Security delay* - The capability of security delay is met and maintained by SSCs relied on for delay functions and designed to provide assurance of necessary and sufficient time for offsite security response (i.e., licensee proprietary or contract personnel, LE, or combination of licensee and LE) to carry out tactical operations to interrupt (i.e., interdict or neutralize) the DBT adversary from causing radiological sabotage.

6.3.1 The licensee or applicant should design the security delay systems to be appropriately layered for defense-in-depth to achieve the required delay.

6.3.2 Where 10 CFR 73.55(s)(1)(ii) is satisfied for applying the alternative requirement in 10 CFR 73.55(s)(2)(ii), licensees or applicants should incorporate security delay systems in the design of a physical protection system to provide sufficient time for LE or other offsite armed responders to interdict and neutralize threats up to and including the DBT of radiological sabotage.

6.3.3 To provide adequate delay, licensees or applicants should design their security systems to be able to delay the DBT for a time equal to or greater than a site's SBT, based on the process described in Appendix C, "Security Bounding Time and Adversary Interference Precluded Time," of this guidance.

6.4 *Delay system and protecting against DBT coordinated vehicle bomb assault* - 10 CFR 73.1(a)(1)(iii) and (a)(1)(iv) establish the DBT capability of land and waterborne vehicle bomb assault, which may be coordinated with an external assault.

6.4.1 The licensee or applicant should design its physical protection program relying on LE or other offsite armed contingency response to protect the plant from the DBT coordinated vehicle bomb assault.

6.4.2 If security responders are not available on site to prevent the DBT from defeating typical barrier systems that are installed at a minimum safe stand-off distance, and if engineered delay systems do not provide sufficient delay for an offsite response force to arrive before the DBT can complete its tasks, then the licensee or applicant should design and configure the structures housing the reactor, spent fuel, and other inventory of radiological material to withstand the effect of the DBT vehicle bomb.

6.4.3 The facility SSCs required for safety and barriers containing radiation hazards should have a hardened structural design to protect against blast pressures and/or be located sufficiently below ground to withstand DBT vehicle bomb blast effects.

6.4.4 Applicants should refer to NUREG/CR-7201, "Characterizing Explosive Effects on Underground Structure," for methods of characterizing the effects of explosions on underground structures resulting from explosive charges located close to and on the ground surface.

6.5 Memorandum of understanding (MOU)

6.5.1 A licensee relying on LE should document and maintain agreements with applicable LE agencies that are willing and capable of providing armed response. The MOU agreement should establish the mutually agreed upon commitments and the LE agency's acceptance of performing interdiction and neutralization functions to defend the licensed facility. The safeguards details of how LE will response to contingency events should be described in the license's safeguards contingency plan. The MOU should include the following:

6.5.1.1 The mutually agreed upon commitments should include both the licensee and LE's activities to plan, train, drill, and exercise contingency response to ensure LE can respond to interdict and neutralize the DBT at all times.

6.5.1.2 The mutually agreed upon commitments should identify the planning and preparedness activities to ensure reliability and availability of LE responses to interdict and neutralize the DBT.

6.5.2 The following activities should be considered for LE contingency responses:

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

6.5.3 The MOUs should include specific commitments of LE resources (people and equipment) that will be available and the minimum response times needed for LE to respond and successfully interdict and neutralize the DBT adversary.

6.5.4 The MOUs should include mutually agreed upon frequencies for LE-related activities in support of licensee drills and exercises. Licensees must meet the frequency of tactical response drills and force-on-force exercise requirements in Appendix B, section VI.C.3.(l)(1) to 10 CFR Part 73.

6.5.5 The licensee MOU with LE should capture response contingencies that may affect the availability of LE to respond, such as LE budgetary constraints, events that would likely compete for resources, or ongoing responses other than to a licensee plant.

6.5.6 The licensee should identify any mutual aid agreements for sharing resources between LEs that may be applied in such contingencies in the MOU.

6.5.7 The licensee should establish additional MOU with any mutual aid LE agencies that may be relied on to respond to a DBT attack.

6.5.8 To maximize the likelihood that the required LE assistance will be available and reliable at all times, a licensee should consider establishing MOUs with at least two LE agencies that have not entered into a mutual aid agreement with each other and that are independently capable of interdicting and neutralizing the DBT.

6.6 Management measures crediting LE response

6.6.1 A licensee applying the alternative requirement in 10 CFR 73.55(s)(2)(ii)(A) remains responsible for assuring that the capability to interdict and neutralize the DBT for radiological sabotage is maintained.

6.6.2 For the reliance on LE agency or agencies, the physical protection program should establish policies, processes, procedures, and an organization for implementing the committed activities mutually agreed to in MOUs with all LEs.

6.6.3 A licensee should document in its PSP and SCP the security licensing basis for how LE response will be relied on to perform interdiction and neutralization functions.

6.6.4 The PSP and SCP should describe how the LE agency or agencies will provide the necessary response to implement contingency responses to achieve the performance objectives and meet the requirements of 10 CFR 73.55(b).

6.6.4.1 The descriptions should capture specific LE capabilities, including but not limited to, the minimum number and positions (i.e., patrol officer, tactical team member) of available responding LE officers, response equipment, tactical capabilities, and response times, and the relevant plant structures and systems required for providing delay.

6.7 Licensee's Safeguards Contingency Plan

10 CFR 73.55(c)(5), "Safeguards Contingency Plan," states, "The licensee shall establish, maintain, and implement a Safeguards Contingency Plan that describes how the criteria set forth in appendix C, section II, to this part, 'Nuclear Power Plant Safeguards Contingency Plans,' will be implemented."

6.7.1 A licensee applying the alternative requirement in 10 CFR 73.55(s)(2)(ii)(A) of relying on LE or other offsite armed responders to fulfill the interdiction and neutralization functions required by 10 CFR 73.55(b)(3)(i) must meet the requirement of 10 CFR 73.55(c)(5) for a (SCP) and is not relieved from the requirements in appendix C, section II except for the requirement in section II.B.3.c.(iv).

6.7.2 The licensee must document and describe how LE or other (i.e., licensee proprietary or contract) offsite armed response personnel will implement the licensee's physical protection program to defend against threats to its facility, up to and including the DBT of radiological sabotage.

6.7.3 The SCP should describe in sufficient detail how the alternative of relying on LE or other offsite armed responders to perform interdiction and neutralization functions, in lieu of onsite licensee personnel, will achieve the goals of the licensee SCP to:
(1) organize the response effort using LE or licensee personnel,
(2) provide predetermined, structured response by LE and licensees to safeguards contingencies,
(3) ensure the integration of the LE and licensee response and other offsite entities, and
(4) achieve a measurable performance in response capability.

6.7.4 The SCP should describe the planning and organizing of the LE and the licensee's resources in such a way that the LE responders (i.e., participants) will be identified, their responsibilities specified, and the responses coordinated. The SCP should also describe what constitutes a timely LE response, indicate LE responders and licensee contingency response personnel training and qualification, and detail how coordination between LE responders and licensee contingency response personnel will be accomplished.

6.7.5 The SCP should describe how the requirements set forth in 10 CFR 73, appendix C, section II, will be implemented when relying on LE or other offsite armed responders to fulfill the interdiction and neutralization functions in 10 CFR 73.55(b)(3).

6.7.6 The licensee should provide descriptions of how the LE agency or other offsite armed responders will fulfill interdiction and neutralization of threats up to and including the DBT of radiological sabotage in the SCP. These descriptions should be maintained as the

licensing basis justifying the alternative of relying on LE, instead of licensee onsite armed responders, to fulfill interdiction and neutralization functions.

6.7.7 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).[2] These systems, components and facility configuration must ensure that LE has 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.

6.7.8 In order to meet the requirements of 10 CFR 73.55(c)(5), the SCP should include descriptions of the activities described in the licensee's MOU with the LE agency and the LE agency's LECR. The LECR should be maintained independent of the licensee security plan (i.e., physical protection, training and qualification, safeguards contingency, and cyber security) 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 sabotage of the plant to cause release of radiation hazards that would endanger the public.

6.7.9 The licensee should describe management measures and controls in the SCP to include the management and control of changes to the MOU with any LE agency that is relied upon to fulfill the interdiction and neutralization functions.

6.7.10 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 LE-related activities.

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

6.8 Contingency response planning and implementation

6.8.1 A licensee should establish appropriate frequencies for conduct of planning and implementation of contingency responses activities with LE agencies for assuring the capabilities to carry out interdiction and neutralization functions as committed to through the MOU.

6.8.2 The licensee should ensure that tactical response drills and force-on-force exercises are conducted in accordance with the requirements of Appendix B, Section VI.C.3.(l)(1) to 10 CFR Part 73.

6.8.2.1 When the licensee relies on LE 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

[2] A LECR is a law enforcement-developed and -controlled plan. For awareness, LECR is just one label for the plan, or set of plans, that law enforcement may develop to guide its contingency response to a power reactor site. When a licensee relies on law enforcement to interdict and neutralize the DBT adversary, the licensee should align its Safeguards Contingency Plan with whatever law enforcement calls its response plan(s).

conducted in a manner to make them available to the LE agency. The licensee should conduct a sufficient number of security drills and exercises to enable LE armed responders who may implement contingency response and licensee protective strategy to participate in the licensee-conducted drills and exercises.

6.8.2.2 When the licensee relies on other (i.e., licensee proprietary or contract) offsite armed responders to perform the interdiction and neutralization function, the licensee should ensure that all armed responders who may implement contingency response and licensee protective strategy participate in licensee-conducted security drills and exercises.

6.8.2.3 Licensee conducted security drills and exercises are performed at the following minimum frequencies:

- Tactical response drills – quarterly
- Force-on-Force exercise – annually

6.8.3 The licensee should conduct the following emergency response preparedness activities with a minimum frequency as indicated below:

- Provide plant familiarization and walkdown – 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.

- Test communications – twice daily, morning and afternoon.

6.8.4 These frequencies are important because they help to establish reasonable assurance that the LE will be reliable and prepared to respond to a DBT attack. The licensee should incorporate these frequencies into applicable site policies, processes, and implementing procedures.

6.8.5 Consistent with Section 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 FOF exercise.

6.8.6 Appendix B, Section VI.C.3.(a) to 10 CFR Part 73, requires that licensees shall 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 the armed response relied on to carry out interdiction and neutralization functions during safeguards contingency events.

6.8.7 Acceptable methods for conducting tactical response drills and FOF exercises for assuring and demonstrating the effectiveness of LE responders to interdict and neutralize the DBT adversary are described in the following appendices of this guidance:

- Appendix A, "Conduct of Law Enforcement Contingency Response Drills"
- Appendix B, "Conduct of Law Enforcement Contingency Response Force-on-Force Exercise"

6.9 No licensee security responders for interdiction and neutralization

6.9.1 A licensee that satisfies the requirements in 10 CFR 73.55(s)(1) may design its physical protection program to adequately perform the required security detection, assessment, and delay functions and then rely on LE to interdict and neutralize the DBT.

6.9.2 A licensee that adopts such an approach should establish the necessary and sufficient management system and controls, including security organization, to oversee all of these security functions, including the LE response.

6.9.3 The licensee, having satisfied the requirements in 10 CFR 73.55(s)(1), is relieved of the requirements in 10 CFR 73.55(k)(3) through (7) relating to armed response personnel, and because the licensee is relying on LE to interdict and neutralize the DBT, is relieved from the requirement in 10 CFR 73.55(k)(8)(ii).

6.10 Licensee with onsite or other (i.e., licensee proprietary or contract) offsite security responders for interdiction and neutralization

6.10.1 Except for relief from 10 CFR 73.55(k)(5)(ii), the licensee must comply with the requirements in 10 CFR 73.55(k)(3) through (7) and 10 CFR 73.55(k)(8)(ii) for the licensee's onsite security personnel and/or other (i.e., licensee proprietary or contract) offsite security responders who implement its physical protection program.

6.10.2 When a licensee relies on offsite proprietary or contract armed responders to interdict and neutralize the DBT adversary, the licensee should house the full number of responders who are needed to adequately defend against the DBT in at least two separate offsite locations. This arrangement will provide defense in depth and ensure the continuous availability and reliability of the offsite response.

6.10.2.1 The licensee should establish 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.

6.10.2.2 Considerations should include protection against:

- Unauthorized access by personnel or vehicles,
- Disruption of communications,
- Delay or blockage of the facilities' egress routes.

6.10.3 In accordance with the provisions of 10 CFR 73.55(c), the descriptions of how requirements are implemented must be documented in the licensee's security plans (i.e., the PSP , training, and qualification plan, SCP , and cyber security plan).

7. Compensatory measures for a degradation or absence of law enforcement or other offsite armed responders

10 CFR 73.55(s)(2)(ii)(A)(*5*) states that *the licensee must identify criteria and measures to compensate for the degradation or absence of law enforcement or other offsite armed responders and propose suitable compensatory measures that meet the requirements of paragraphs (o)(2) and (3) of this section to address this degradation.*

7.1 The licensee should develop compensatory measures for the degradation or absences of LE or other offsite armed responders to fulfill the interdiction and neutralization functions to be consistent with 10 CFR 73.55(o)(2) to ensure that the compensatory measures will provide an equivalent level of protection.

7.1.1 One straightforward method to meet the equivalency requirement when relying on LE to fulfill the interdiction and neutralization functions, is for a licensee to coordinate, plan, and train with at least two LE agencies that independently 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 agency when the licensee becomes aware that the support needed from the primary LE agency is degraded or unavailable.

7.2 Consistent with 10 CFR 73.55(o)(3), a licensee should have compensatory measures to be implemented within the specific timeframe needed to ensure that the situations resulting from the degradation or loss of capabilities from absence of offsite safeguards contingency responses cannot be exploited.

7.2.1 A licensee should identify possible situations that could result in the unavailability of its LE or other offsite armed responders. The licensee's compensatory measures should include identification of the alternative measures and the timeframe for implementation of those measures to prevent loss of interdiction and neutralization functions and should be described in the PSP

7.2.2 The licensee should establish criteria for when to implement the compensatory measures addressing the possible situations where the LE or other offsite armed responders may be unavailable or only capable of providing a limited response to fulfill the interdiction and neutralization functions of contingency responses.

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

7.3.1 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.

7.3.2 The considerations of how adversely the degraded situations affect interdiction and neutralization functions should determine the equivalent compensatory measure that the licensee must implement. One acceptable approach could be to provide response by 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.

7.3.3 Procedures for evaluating the measures should take into consideration the safety/security interface requirements of 10 CFR 73.58, including plant configurations and facility conditions.

7.3.4 This evaluation should be focused 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.).

7.4 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).

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

7.4.2 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.

7.5 The purpose of a compensatory measure evaluation is to ensure that the integrity of the licensee's physical protection program is not reduced beyond acceptable standards and that the contingency response capabilities are maintained to achieve the physical protection program's overall performance objective and meet the requirements of 10 CFR 73.55(b).

7.6 Using a compensatory measures evaluation, licensees may 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.

7.6.1 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.

7.6.2 For example, a licensee's capabilities to assess, detect, delay, interdict and neutralize should be maintained through the implementation of compensatory measures.

7.7 In determining the proper application of appropriate compensatory measures in a situation of degradation of LE or other offsite armed responders, the licensee should consider the use and application of all security assets with the minimum standard complement of security staffing.

7.7.1 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.

7.8 The results of a compensatory measures evaluation may demonstrate the need for additional staffing at a certain time or during certain situations.

7.8.1 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.

7.9 Immediate measures provide a level of response to a degradation or loss of functions to minimize the possible exploitation until longer term measures can be taken.

7.9.1 Consistent with 10 CFR 73.55(o)(2), compensatory measures must provide an equivalent level of protection until the degradation or loss of f interdiction and neutralization functions is corrected.

7.9.2 Consistent with 10 CFR 73.55(o)(3), compensatory measures must be implemented within specific time frames necessary to meet the requirement of 10 CFR 73.55(b).

7.9.3 To satisfy these requirements, the compensatory measure that provides an equivalent level of protection should be in place within the appropriate time frame based on the licensee's evaluation of the significance of the degradation.

7.10 When degradation consisting of the absence of LE 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.

8. Alternative requirements for physical barriers

10 CFR 73.55(s)(2)(iii) states that a *licensee that meets* 10 CFR 73.55*(s)(1) may utilize means other than physical barriers and barrier systems to satisfy the physical protection program design requirements of* 10 CFR 73.55*(e). Acceptable means can be any method(s) that accomplishes the delay and access control functions necessary to allow the licensee to implement its physical protection program.*

8.1 Engineered passive or active barrier systems

8.1.1 Alternative means of providing security delay or access control functions that meet the performance objective and requirements of 10 CFR 73.55(b) may be in the form of active and passive engineered systems other than the physical barriers defined in 10 CFR 73.2, which specifies the design of fences and the construction of building walls, ceilings, and floors.

8.1.2 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.

8.1.3 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.).

8.1.4 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.

8.1.4.1 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 SBT, based on the process described in Appendix C, "Security Bounding Time and Adversary Interference Precluded Time," of this guidance.

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

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

8.1.4.4 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.

8.1.5 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.

8.1.5.1 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.

8.1.5.2 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.

8.1.5.3 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.

8.1.6 A licensee should design physical barriers to satisfy the requirements of 10 CFR 73.55(e). The licensee may use the acceptance criteria in SRP Sections 13.6.1 and 13.6.2 to assist in the design of physical barriers.

8.1.7 In order to satisfy the analysis requirement in 10 CFR 73.55(s)(1)(iv) the licensee should describe in sufficient detail the specific use, type, function, and placement of physical barriers needed in a physical protection system designed to protect against the DBT adversary to achieve the requirements in 10 CFR 73.55(b) and needed to implement elements of a physical protection program in accordance with requirements in 10 CFR 73.55.

8.1.8 In order to satisfy the requirements of 10 CFR 73.55(c), the licensee should describe and capture the design and implementation of an alternative physical barrier system as part of the facility security licensing basis.

8.1.9 The licensee should describe in sufficient detail in the security plans how the engineered and administrative controls, management systems, and organization meet the requirements in 10 CFR 73.55.

8.1.10 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.

8.1.11 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.

8.1.12 The licensee should design the configuration of physical barrier systems for access controls to satisfy the requirements of 10 CFR 73.55(g). 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.

8.1.13 Physical vehicle barrier system designs, typically installed at currently operating power plants, are designed and installed to prevent vehicles from entering (or leaving) and may consist of passive (fences, walls, concrete blocks, concrete and sand barriers, shallow vehicle barriers, etc.) and active (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 (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.

8.1.14 In accordance with 10 CFR 73.55(e)(1)(ii), the use of alternative physical security requirements using means other than physical barriers as defined in 10 CFR 73.2 must be described in the PSP. In accordance with 10 CFR 73.55(e)(2), the licensee is required to retain, in accordance with 10 CFR 73.70, “Records,” all analyses and descriptions of the physical barriers and barrier systems used to satisfy the physical protection program

design requirements of 10 CFR 73.55(e). The descriptions of how physical barriers are applied in the design of a physical protection program to provide delay functions (i.e., the details of analyses supporting the design of the alternative means to achieve the intended delay functions, the locations, and specific details, including implementing procedures) are considered safeguards information and must be protected in accordance with the requirements of 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements."

9. Alternative requirements for secondary alarm station

10 CFR 73.55(s)(2)(iv) states a licensee that meets paragraph (s)(1) of this section:

(A) May have one alarm station located offsite notwithstanding the requirement in paragraph (i)(2) of this section to have at least two alarm stations located onsite. The central alarm station must remain onsite.

(B) With a secondary alarm station located offsite, is relieved from the requirement in (i)(4)(iii) of this section to construct, locate, and protect the offsite alarm station to the standards for the central alarm station. The licensee is not relieved from the requirement in (i)(4)(iii) that both alarm stations shall be equipped and redundant, such that all functions needed to satisfy the requirements of paragraph (i)(4) of this section can be performed in both alarm stations.

9.1 This alternative requirement permits a licensee that meets 10 CFR 73.55(s)(1) to design a physical protection program with a secondary alarm station located offsite.

9.1.1 The alternative requirement provides relief from compliance with the construction, location, and protection requirements in 10 CFR 73.55(i)(4)(iii) for an offsite secondary alarm station.

9.1.2 In addition, the requirements in 10 CFR 73.55(i)(4)(i)(D) and 10 CFR 73.55(i)(4)(ii)(A) related to constructing, locating, and protecting an offsite secondary alarm station would not be applicable for a secondary alarm station that is located offsite.

9.2 The licensee's design of its secondary alarm station is required to be equal and redundant with all functions performed in a secondary alarm station located onsite.

9.2.1 The licensee should identify the required security functions of the secondary alarm station for implementing the physical protection program and meeting the applicable requirements in 10 CFR 73.55.

9.2.2 An offsite secondary 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 LE assistance, and
- communicating with onsite/offsite security to assist implementing the security response.

9.2.3 Equipment in the central and secondary alarm stations does not have to be identical. However, both alarm stations must have the same functional capabilities.

9.3 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 secondary alarm station offsite should include the systems and components for assuring reliable remote operation and control of access, delay barriers, and security systems.

9.4 The licensee's secondary alarm station 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's central alarm station and LE agencies or other offsite armed responders.

9.4.1 Communications and control systems should be designed to be designed to address the ability of the DBT adversary to interrupt or interfere with the continuity or integrity of communications.

9.4.2 The design should apply the principles of redundancy and diversity.

9.5 A licensee may use a monitoring service to fulfill the security functions that should be performed by a secondary alarm station.

9.5.1 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 73.55(b).

9.6 For a secondary alarm station that is designed 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.

9.7 The descriptions in the design and security licensing bases should capture the application and implementation of the alternative requirement that permits a secondary alarm station to be located offsite.

9.7.1 The descriptions of the offsite secondary alarm station should satisfy the requirement in 10 CFR 73.55(c), where the security plans (consisting of a PSP, T&QP, SCP, and CSP) adequately describe in sufficient detail how engineered and administrative controls, management systems, and organization meet the requirements in 10 CFR 73.55.

10. Alternative requirements for vital areas

10 CFR 73.55(e)(9)(v) states that *at a minimum, the following shall be considered vital areas:*
(A) The reactor control room;
(B) The spent fuel pool;
(C) The central alarm station; and
(D) The secondary alarm station in accordance with § 73.55(i)(4)(iii).

10 CFR 73.55(e)(9)(vi) states that *at a minimum, the following shall be located within a vital area:*

(A) The secondary power supply systems for alarm annunciation equipment; and
(B) The secondary power supply systems for non-portable communications equipment.

10 CFR 73.55(s)(2)(v) states that *a licensee that meets 10 CFR 73.55(s)(1):*

- *is relieved from the requirement in paragraph (e)(9)(v)(D) of this section to designate an offsite secondary alarm station as a vital area.*
- *is relieved from the requirement in paragraph (e)(9)(vi) of this section to locate the secondary power supply systems for an offsite secondary alarm station in a vital area.*

Clarifications:

10.1 In addition to being relieved of the requirement to designate the offsite secondary alarm station as a vital area [per 10 CFR 73.55(e)(9)], the prescribed vital area protection requirements would no longer be applicable to a secondary alarm station located offsite.

10.2 A licensee would no longer be required to comply with the prescriptive requirements for physical barriers, target sets, access controls, and detection and assessment that would normally be associated with a secondary alarm station vital area pursuant to subsections 10 CFR 73.55(e), 10 CFR 73.55(f), 10 CFR 73.55(g), and 10 CFR 73.55(i), respectively.

11. 10 CFR 73, Appendix B, Section VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties"

10 CFR 73, Appendix B, Section VI.A.1. states:

For light-water reactors, other than small modular reactors, as defined in 10 CFR 171.5 of this chapter, the licensee shall ensure that all individuals who are assigned duties and responsibilities required to prevent significant core damage and spent fuel sabotage, implement the Commission-approved security plans, licensee response strategy, and implementing procedures, meet minimum training and qualification requirements to ensure each individual possesses the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities.

For small modular reactors, as defined in 10 CFR 171.5 of this chapter, or for non-light-water reactors, the licensee shall ensure that all individuals who are assigned duties and responsibilities required to prevent a significant release of radionuclides from any source, implement the Commission-approved security plans, licensee response strategy, and implementing procedures, meet minimum training and qualification requirements to ensure each individual possesses the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities.

11.1 A licensee training and qualification program for licensee security personnel should conform to RG 5.75.

11.2 On the basis that LE responders are trained and qualified at a level that is equivalent to or greater than that required by Appendix B, the requirements do not apply to LE personnel who a licensee relies on to perform interdiction and neutralization functions.

D. IMPLEMENTATION

The NRC staff may use this RG 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 RG to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 50.109, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," (Ref. 30), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." 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.

ACRONYMS/ABBREVIATIONS

The following abbreviations are used in this RG:

ADAMS	Agencywide Documents Access and Management System
AIPT	Adversary Interference Precluded Time
CAS	central alarm station
CFR	Code of Federal Regulations
CSP	cyber security plan
COL	combined license
DBT	design basis threat
DE	dose equivalent
DG	draft regulatory guide
FOF	force on force
FSAR	final safety analysis report
IAEA	International Atomic Energy Agency
LE	law enforcement
LECR	law enforcement contingency response plan
LLEA	local law enforcement agency
LWR	light-water reactor
MAF	mock adversary force
MILES	Multiple Integrated Laser Engagement System
MOU	memorandum of understanding
NRC	U.S. Nuclear Regulatory Commission
OMB	Office of Management and Budget
OL	operating license
PRA	probabilistic risk assessment
PSP	physical security plan
RG	regulatory guide
SAR	safety analysis report
SAS	secondary alarm station
SCP	safeguards contingency plan

SBT	security bounding time
SGI	safeguards information
SMR	small modular reactor
SRP	Standard Review Plan
TEDE	total effective dose equivalent
T&QP	training and qualification plan

Appendix A to DG 5072
Conduct of Law Enforcement
Contingency Response Drills

1 OVERVIEW

1.1 Regardless of whether licensees elect to rely on LE or other offsite armed responders to interdict and neutralize the DBT adversary, licensees are required to establish, implement, and maintain a performance evaluation program consistent with the requirements in Section VI.C.3 of Appendix B to 10 CFR Part 73. 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.

1.1.1 When relying on proprietary or contract armed security responders to interdict and neutralize the DBT adversary, licensees should follow the security drill and exercise guidance in the Performance Evaluation Program Section (i.e., Section 5) of RG 5.75.

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

1.1.2 When relying on LE responders to interdict and neutralize the DBT adversary, licensees should follow the guidance in Appendices A and B of this publication.

1.1.2.1 The guidance in Appendices A and B is similar to that in RG 5.75, but it has been modified to account for the different considerations that will exist when relying upon LE responders rather than licensee-controlled security personnel.

1.2 This guidance establishes performance objectives and provides an overview of one recommended method for the planning and execution of both a Tabletop Exercise (TTX) and Limited Exercise (LX) addressing the site-specific LE agency contingency response at an operating nuclear power reactor.

1.2.1 Consistent with Section 1.4 below, LE TTXs and LXs are two acceptable methods that licensees can use to satisfy the quarterly tactical response drill requirement in Section VI.C.3.l.(1) of Appendix B to 10 CFR Part 73.

1.3 The objectives and outcomes of exercising the protective strategies in the law enforcement contingency response (LECR) plan should be to 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 Tabletop drills are performed to demonstrate the protective strategy using a mockup of the facility. Tabletop drills 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 LE response to contingency events.

1.4.2 Timeline drills are performed to demonstrate the response timelines established for the armed response 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 Limited scope tactical response drills are performed to evaluate the ability of one or more LE or security response force members to effectively implement their protective strategy responsibilities. These drills are conducted as needed for each individual, group, or shift to validate and test the protective strategy.

1.4.4 This is guidance for conducting the LX. The LE LX provides an opportunity to practice the response to a hostile action directed against the licensee's nuclear power plant. An LX should be conducted on a recurring periodic basis to ensure the continued capability to effectively implement the LECR. The frequency of LX recurrence should be agreed upon by the licensee and LE agency (or agencies) in accordance with the minimum required frequencies in Section VI, paragraph C.3.(l)(1) of Appendix B to 10 CFR Part 73.

1.4.5 The licensee SCP should include a description of the activities described in the licensee's MOU with the LE agency and the activities described in the LE agency's LECR. The LECR describes how LE will perform interdiction and neutralization of the DBT adversary. The licensee, in conjunction with the LE agency, 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 LE agency, may warrant additional reviews. Licensees may elect to include this activity as part of their periodic interactions with LE agency.

1.7 While an LE LX has many elements in common with regulatory required security drills and exercises typically involving licensee onsite security forces, there are important differences. To aid in understanding these differences, the key attributes of an LX are listed below.

1.7.1 The LX utilizes as its base document a fully complete, signed, and issued LECR developed through the combined efforts of the licensee and LE agency or agencies, which may include State and Federal agencies.

1.7.2 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 SSCs for LE operational planning and contingency responses to interdict and neutralize threats.

1.7.3 The LX 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.

1.7.4 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.

1.8 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.

1.9 Licensee's operations personnel should provide information on any plant safety and security priorities (which will lead to specific LE response) or support LE response related to the planning of on-site tactical operations.

1.10 The conduct of an LX 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.

1.11 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.

1.12 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, LX constraints may require that certain events, consequences, or response actions be embellished or presented in a time-compressed fashion. LX participants should be made aware of these stipulations, and of the expectation to assess, and respond to, the events as presented.

1.13 LX 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 PSP and SCP.

1.14 The NRC recognizes the LE 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 LX.

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 LX 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 LX should include:

2.2.1. Ensuring an understanding of the tactical integration components of the LECR, including a review of the expected process for Identifying Friend or Foe (IFF)[3] and accessing the plant (e.g., owner controlled area (OCA), protected area (PA), vital areas (VA)).

2.2.2. Providing an opportunity for LE 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. Demonstrating the communication systems, components, processes, and procedures anticipated to be used to support LE tactical operations under actively hostile conditions, including a radiation hazards environment.

2.3 Additionally, Attachment 1 to this Appendix, *Recommended LECR Limited Exercise Objectives*, presents generic guidance that a site should use to develop a set of LX 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 LX performance should include a review of past performance objectives and outcomes.

2.5 The licensee, with LE participation, should critique TTX and LX 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 LX. Each item should be reviewed, and identified actions incorporated into the appropriate LX 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 LX. 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 LX 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] Identifying Friend or Foe (IFF) - A system developed and recognized between the licensee site personnel and response forces to distinguish themselves from enemy forces.

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

3.2 EXERCISE SUPPORT FROM SECURITY

3.2.1 Licensee safety and security is critical to the successful development and execution of the LX. Safety and security personnel provide valuable direction and assistance to exercise participants in the following areas.

(1) Verifying protection of Safeguards Information in LX materials or during the LX.

(2) Assuring knowledge of safety and security-related procedures, equipment, and timelines.

(3) Developing credible DBT attack sequences, and related reports and indications.

(4) Devising methods to simulate response actions and communications with safety and security facilities and licensee personnel.

(5) Facilitating LX planning and preparation with LE (local, State, and Federal) personnel.

(6) Providing knowledgeable controllers for safety and security facilities/functions.

(7) Verifying no plant safety operational impact from LX performance.

(8) Establishing credible operational objective for LX contingency response planning.

(9) Validating LE agency 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 LX TOC should be established in a location that would actually be used during a real event, and not one selected primarily to facilitate LX performance. LX 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 LX). The conduct of communications systems testing prior to the LX 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.

(1) 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 LX scenario.
(2) 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.
(3) 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

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

3.6 LECR TABLETOP EXERCISE

3.6.1 The licensee should perform an LE TTX with the participating LE agency or agencies identified in the LECR prior to the initial LX and on a periodic basis not longer than every three years. A TTX provides LE personnel 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 6.0, *LECR Tabletop Exercise Implementation*, and Attachment 2, *Tabletop Exercise Guidelines*, of this Appendix 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 LE response 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, LE agency, and other applicable agencies should be used. This should include decision-makers of the local, State, and Federal responds agencies. The licensee should engage LE personnel early in the scenario development process to define and discuss scenarios, events, and challenges and to confirm LE agency participation in the upcoming exercise.

4.2 SAFEGUARDS/SECURITY SENSITIVE INFORMATION

4.2.1 LE 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 LE; however, caution should be used to ensure that SGI is protected and not released to unauthorized personnel.

4.2.2 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.

4.3 SCENARIO DEVELOPMENT AND KEY ATTRIBUTES

4.3.1 When developing an LX scenario, the first decision to be made is whether the attack will consist of a standalone insider, cyber attack, 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.

4.3.2 Figure 4-1, *Framework for an Offsite Law Enforcement Agency Contingency Response Limited Exercise*, presents recommended frameworks for developing an LX 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.

4.3.3 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.

4.3.4 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.

4.3.5 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.

4.3.6 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 LE agency 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.

4.3.7 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.

4.4 SCENARIO TIME PROGRESSION

4.4.1 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.

4.4.2 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.

4.5 MINI-SCENARIOS / MASTER SCENARIO EVENTS LIST DETAIL DESCRIPTIONS

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

4.5.2 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 shall not use actual attack progression timing as described in security program documents; however, the selected event sequence and times should be credible.

4.6 EXERCISE SCENARIO CONFIDENTIALITY

4.6.1 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 LX. 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 response.

4.6.2 Players should not know any details of the scenario (i.e., specific event timeline and related information). The scenario used for an LX should be sufficiently different from that used in the immediately preceding TTX and/or LX. 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.

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

FIGURE 4-1

Framework for an Offsite Law Enforcement Agency Contingency Response Limited Exercise

Initial Response Phase	Continued Response Phase
• LE agencies and licensee 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) • LE and 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 LE agencies 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 LX; 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 LX should demonstrate a coordinated response by LE personnel. To effectively demonstrate this objective, a simulated Central Alarm Station (CAS) and Secondary Alarm Station (SAS) can be established (i.e., a control cell) for initiating LE 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 the LE response personnel, 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 LECR TABLETOP EXERCISE IMPLEMENTATION

6.1 Prior to conducting an initial LECR LX, 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, *Tabletop Exercise Guidelines*, for preparation and execution of a TTX. The frequency of TTX recurrence should be agreed upon by the LE agency or agencies relied on for contingency response, including any supporting LE agencies.

6.3 TTX participants should include, at a minimum: (i) LE executives (e.g., Chiefs, Sheriffs, 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; (ii) LE tactical team commanders; and (iii) 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: (i) at the implementation of a LECR , or when more than 25% of LE executive participants change (e.g., due to retirement, promotion, etc.), whichever occurs first and (ii) in accordance with drill and exercise requirements established in Section VI, paragraph C.3.(l)(1) of Appendix B to 10 CFR Part 73.

6.5 The licensee should ensure that a TTX is designed to: (i) validate whether existing policies, procedures, and interagency/inter-jurisdictional agreements are sufficient for contingency response; (ii) familiarize responding LE personnel with important concepts (e.g., implications of site focus changing from individual safety to public health and safety, how LE response fits into contingency response, and applicability of LE response paradigms, deadly force considerations, etc.) and current or expected capabilities or actions related to a sabotage attack; and (iii) 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.

TTX and LX action items are tracked, dispositioned, and captured as lessons learned when appropriate. Results from the tabletop exercises are used to update and validate the LECR. The licensee should ensure LE 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. The LE tactical teams identify and test viable primary, secondary, and tertiary communications systems and protocols for drills and exercises.

Appendix A to DG 5072
Attachment 1
LECR Limited Exercise Objectives

LECR Limited Exercise Objectives

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.

Appendix A to DG 5072
Attachment 1
LECR Limited Exercise Objectives

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.

Appendix A to DG 5072
Attachment 1
LECR Limited Exercise Objectives

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.

Appendix A to DG 5072
Attachment 2
Tabletop Exercise Guidelines

Tabletop Exercise Guidelines

1. INTRODUCTION

1.1 The LECR Tabletop Exercise (TTX) provides a facilitated learning environment for key licensee personnel, and offsite LE agencies, to review and discuss their respective roles and responsibilities. The TTX helps ensure the practicality and effectiveness of the licensee's LECR plan. In particular, it 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 LE 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 LE response, immediate radiation hazard concerns, and protection of equipment important to safety. Likewise, the licensee will gain an appreciation for LE 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, offsite LE armed responders, and finally other offsite response personnel.

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 LECR-based event. This understanding should contribute to a successful response during the LX. The Exercise Manager should consider the following topics for inclusion in the tabletop agenda.

(1) Method(s) used by the site to notify offsite first responders of a threat and/or attack.

(2) Method(s) for subsequent dissemination of this information among offsite response organizations.

(3) Initial site safety/security actions in response to the DBT event.

(4) Initial offsite LE armed responder actions upon notification:

(a) Site access requirements for offsite LE armed responders
(b) Staging and/or reporting location(s) of LE armed responders
(c) Communications and coordination with Incident Commander (IC) and site security

2.2 Establishment of the Tactical Operations Center (TOC):

(1) Who oversees the overall response, and how would transitions in command and control take place as the scenario evolves?

(2) Key support personnel reporting to the TOC and their respective functions

(3) How would offsite armed responders obtain turnover from, and integrate with, the site response?

(4) How will IC communicate and coordinate with on-site decision-makers?

2.3 Radiation protection provisions for offsite LE armed responders to the site

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

2.5 Coordination and decision-making related to:

(1) Ensuring that the TOC understands operational priorities for operation of functional equipment or restoration of damaged plant equipment

(2) 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:

(1) Date, time, and location

(2) What individuals from the site and key offsite response organizations will be invited to participate in the TTX

(3) 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 offsite LE 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:

(1) Given the scenario, determine what the agencies perceive as their role and extent-of-play

(2) Determine what the agencies want to learn from the TTX as a guide for the facilitator

(3) Determine which LE agencies and supporting agencies will have a lead and supporting role at different stages of the timeline

(4) Provide the LE and other agencies the opportunity to think about their individual extents-of-play as the tabletop scenario evolves and how the command structure may change

(5) Establish ownership, among key offsite participants, of respective roles in the tabletop

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., 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 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 offsite LE 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:

(1) Information requirements of each organization and how communications will occur among facilities and organizations.

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

5 CRITIQUE AND FOLLOWUP

5.1 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 tabletop 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.

Appendix A to DG 5072
Attachment 2
Tabletop Exercise Guidelines

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

	• Discussion topics involve multiple functions and considerations (e.g., communications, staging 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	

Appendix A to DG 5072
Attachment 2
Tabletop Exercise Guidelines

Response Validation Options	Benefits	Challenges/Limitations
Limited Exercise	• 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 • 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,	• 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 • 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

	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)	• 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.

Response Validation Options	Benefits	Challenges/Limitations
Full-Scale Exercise with laser engagement equipment	• Includes elements from the LX Benefits • Involves a larger number of 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 LE weapons fire, heat, noise, radiation, interior complexity of site, communications challenges) • Necessitates sound tactical plans and movements • Laser engagement equipment provides the realistic tactical stimuli to which LE team members can respond, instead of responding to verbal information or a written inject. • Can identify potential incidences of fratricide or lessons learned on how to avoid them in the future	• Includes appropriate elements from the LX Challenges/Limitations • Adds additional layers of complexity to the exercise • Using controllers as adversaries vice an adversary team to maximize the training value for LE 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 LE 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, dealing with everything 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

		• 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 B to DG 5072
Conduct of Law Enforcement Contingency Response
Force-On-Force Exercises

1. Performance Evaluation Program

1.1 Section VI, paragraph C.3.(a) of Appendix B to 10 CFR Part 73, requires that licensees shall 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 the LE response relied on 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 LE responders to interdict and neutralize the DBT adversary are described in this guidance.

1.2 To satisfy the requirements of Section VI, paragraph C.3 of Appendix B to 10 CFR Part 73, a licensee that relies upon LE 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 LE response to contingency events . These drills and exercises are vital components of a comprehensive training program that enables the LE responders to gain experience and demonstrate performance of tactics to effectively interdict and neutralize the DBT adversary and perform LE response tasks and activities within the contingency response plan.

2. Tactical Response Force-on-Force Exercises

2.1 The objectives should be: (a) provides opportunities, within a permissive environment, for LE 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; (b) introduces LE tactical teams to several real-world stressors (e.g., hostile environment, heat, noise, radiation, interior complexity of site, communications challenges); and (c) identifies and documents LE command and control and communications capabilities and incorporates those depictions into the LECR.

2.2 Consistent with Section VI, paragraph C.3.(d) of Appendix B to 10 CFR Part 73, licensee FOF exercises (fully integrated, tactical, and limited scope exercises) must 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 LE 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 LE individuals or tactical response teams and they are part of the ongoing training to assure effectiveness of the licensee's SCP and the LECR.

2.3 In accordance with Section VI, paragraph C.3.(f) of Appendix B to 10 CFR Part 73, the scope of exercises conducted for training purposes shall be determined by the licensee and LE; must 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 LE

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. LE 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 RG. Other licensee physical protection program elements, such as insider mitigation, cyber security, access authorization, and inspection, testing, and maintenance of physical security 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 LE 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 LE 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) a fully integrated FOF exercise, (b) a tactical response FOF exercise, and (c) a limited scope FOF exercise. The FOF exercises should be used to exercise both licensee and the 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.

(1) 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.

(2) 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.

(3) 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:

Response Validation Options	Benefits	Challenges/Limitations
Full-Scale Exercise with laser engagement equipment	• Includes elements . from the LX Benefits • Involves a larger number of 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 LE weapons fire, heat, noise, radiation, interior complexity of site, communications challenges) • Necessitates sound tactical plans and movements • Laser engagement equipment provides the realistic tactical stimuli to which LE team members can respond, instead of responding to verbal information or a written inject. • Can identify potential incidences of fratricide or lessons learned on how to avoid them in the future	• Includes elements from the LX Challenges/Limitations • Adds additional layers of complexity to the exercise • Using controllers as adversaries vice an adversary team to maximize the training value for LE 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 LE 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 • 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

2.9 Defining Participation

2.9.1 As described in Section VI, paragraph C.3.(l)(1) of Appendix B to 10 CFR Part 73, licensee personnel assigned duties and responsibilities required to implement the SCP and licensee protective strategy must participate in at least one tactical response drill quarterly and one FOF exercise annually. In addition, as described in 10 CFR 73.55(s)(2)(ii)(A)(*3*) a licensee relying on LE to implement the SCP and fulfill the physical protection interdiction and neutralization functions must make available periodic training to LE 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 LE armed response personnel and make these ongoing training opportunities available to LE personnel to assure effectiveness of the licensee's SCP and the LECR.

2.9.2 In accordance with 10 CFR 73.55(d)(3), the licensee may not permit any individual to implement any part of the physical protection program unless the individual has been trained, equipped, and qualified to perform required interdiction and neutralization functions. As described in Section VI, paragraph C.3.(h) of Appendix B to 10 CFR Part 73, licensees shall document the scenarios and participants for all tactical response drills and annual FOF exercises. Licensees are relieved from the qualification requirements of Appendix B, Section VI, Paragraph D to 10 CFR Part 73, for LE armed responders; however for LE armed responders that participate in tactical response drills and FOF exercises, licensees should document those LE participants.

2.9.3 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.

2.10 Key Program Elements

2.10.1 For licensees that rely upon LE 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.

(1) Responding with the number of LE personnel. The LE agency on which the licensee relies should have the required number of LE response personnel to effectively implement the contingency response.

(2) Responding within the plant delay systems and appropriate LE timelines. LE 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.

(3) Responding to implement tactical operations to defeat DBT adversary blocking measures and impeding force to prevent or delay LE personnel to plant areas. LE personnel use appropriate protection and cover.

(4) Responding LE personnel 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).

(5) Responding LE personnel with appropriate armament. LE personnel are equipped or have readily available the weapons and equipment necessary to execute their tactical operations.

(6) Responding LE command and control structure. LE personnel have appropriate communication capabilities to ensure that decisions and actions are coordinated and communicated in a timely manner to facilitate response. LE communications equipment used to the maximum extent practical; LE Tactical Operations Center (TOC) established to document LE radio communications capabilities and facilitate interoperable communications and route navigation.

2.10.2 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:

(1) coordination and planning.
(2) command and control.
(3) communications.
(4) individual responder tactics.
(5) team response tactics.
(6) use of deadly force.
(7) alarm assessment and intrusion detection.
(8) weapons handling and proficiency.
(9) controller participation.
(10) post-drill briefing and critiques.
(11) integrated response (plant operations, Emergency Preparedness).
(12) deployment of responders and equipment.

2.10.3 Exercise Scenario Development

2.10.3.1 The effectiveness of a drill or exercise as an evaluation tool largely depends on the scenario development phase. To satisfy the requirements of Section VI, paragraph C.3.(d) of Appendix B to

10 CFR Part 73, the proposed scenario must 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. In accordance with Section VI, paragraph C.3 of Appendix B to 10 CFR Part 73, the licensee must develop a scenario to support the conduct of each drill or exercise.

2.10.3.2 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.

2.10.3.3 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:

(1) LE responder timelines and positioning;
(2) impact of changes in the configuration of delay barriers;
(3) temporary modifications to the security plan to support activities that impact the safety/security interface;
(4) effects on fields of fire; or
(5) changes to target sets.

2.10.4 Identification of Target Sets

2.10.4.1 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 LE

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.

2.10.4.2 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 73.55(f), and guidance is described in RG 5.81.

2.10.5 Simulations and Artificialities

2.10.5.1 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.

2.10.5.2 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.

2.10.5.3 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."

2.10.5.4 Simulations and artificialities may apply to both licensee and LE 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.

2.10.6 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:

(1) areas with sensitive plant equipment;
(2) personnel safety;
(3) radiological controls;
(4) foreign material exclusion areas; and
(5) confined space areas.

2.10.7 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 LE participants, the controllers, and the mock adversaries, as well as communicating the conduct of the drill or exercise to onsite and offsite personnel.

2.10.8 Scheduling and Planning

2.10.8.1 As described in Section VI, paragraph C.3.(l)(2) of Appendix B to 10 CFR Part 73, planners must 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.

2.10.8.2 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, LE responders' availability, and FOF tactical exercise requirements.

2.10.8.3 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.

2.10.8.4 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:

1) drill or exercise specifics (number, date, shift/personnel involved, location).
2) pre-notifications (operations, radiation protection, station management, etc.).
3) safety briefings.
4) radiological briefings.
5) specific drill objectives or key elements evaluated.
6) participants (players, controllers, adversaries).
7) adversary characteristics (equipment, tactics, actions taken, target, etc.).
8) scenario being used.
9) sequence of events (event description, anticipated response, estimated timelines).
10) development of a controller matrix (written scenario for controllers) to outline scenario events.
11) simulations and artificialities to be considered or integrated into the evolution safety review.
12) adversary briefings (providing details of the scenario, equipment used, routes, targets, etc., and allowing for intelligence gathering from an insider).
13) controller/evaluator briefings (scenario, assignments, simulations, cautions, concerns, etc.).
14) equipment consideration.

15) initial plant/security status; and
16) what LECR personnel tasks and activities are being tested.

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

2.10.9 Command and Control of Drills and Exercises

2.10.9.1 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.

2.10.9.2 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.

2.10.9.3 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.

2.10.10 Controller Training and Qualification Process

2.10.10.1 As described in Section VI, paragraph C.3.(l)(4) of Appendix B to 10 CFR Part 73, drill and exercise controllers must 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.

2.10.10.2 The goals of the process are the following:

1) establish a common baseline of controller knowledge, skills, and abilities.

2) identify and respond to station and industry controller performance gaps.

3) facilitate peer sharing of controller resources for exercise activities; and

4) provide a feedback loop to support continual improvement in controller performance.

2.10.11 Controller Knowledge and Experience

2.10.11.1 As described in Section VI, paragraph C.3.(l)(4) of Appendix B to 10 CFR Part 73, each controller shall have the knowledge and experience to control and evaluate exercises/drills. This includes the ability to:

(1) 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.

(2) Evaluate the application of the no-play area (to include radiation boundaries) and control measures.

(3) 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.

(4) 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.

(5) Evaluate the tactical use of exercise weapons comprising their effective range and capabilities, including fields of fire.

(6) Evaluate the application of target identification, acquisition, and engagement by players.

(7) Evaluate the tactical use of hand-carried explosive devices on equipment and personnel and their effects upon detonation.

(8) Evaluate the effectiveness of body armor employed by players and its ballistic protection during the exercise.

(9) Evaluate the effectiveness of gas masks, or other supplemental gear, employed during the conduct of the exercise.

2.10.11.2 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:

(1) the use and understanding of the dispersal and effects of chemical agents and smoke grenades.

(2) the gas mask used and its limitations.

(3) the overall procedure for conducting FOF exercises, including the use of Multiple Integrated Laser Engagement System (MILES) equipment.

(4) applicable site-specific delay barriers and movement timelines.

(5) the site's policy on use of deadly force; and

(6) exercise and site safety procedures.

2.10.12 Training Design, Development, and Implementation

2.10.12.1 As described in Section VI, paragraphs C.1.(b) and C.3.(l)(4) of Appendix B to 10 CFR Part 73, all controllers shall complete controller training before participating as a controller in any drill or FOF exercise. As described in Section VI, paragraph D.2 of Appendix B to 10 CFR Part 73, controllers shall be requalified at least annually.

2.10.12.2 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:

(1) procedures, guidelines, and references.
(2) introduction/history.
(3) safety and safe drill play.
(4) communication (primary and alternate).
(5) terminology.
(6) command and control.
(7) providing acquired information to players.
(8) controller knowledge.
(9) position and exercise pace.
(10) rules of engagement and the use of force.
(11) use and effects of explosives.
(12) rules of conduct.
(13) MILES equipment and limitations.
(14) site exclusion areas.
(15) temporary breaks in drill execution.
(16) response team duties.
(17) critique process; and
(18) use and control of safeguards information.

2.10.12.3 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:

(1) drill timeline coordination (situational awareness and proper cue injects).
(2) cover and concealment assessment.
(3) MILES equipment usage and safety.
(4) red (training) gun equipment usage, application, and safety.
(5) use of assigned equipment.
(6) target set equipment.
(7) licensee protective strategy.
(8) simulations related to gas masks.
(9) simulations related to smoke or other chemical agents.
(10) weapons/explosives capabilities and simulation methods; and
(11) safety control.

2.10.12.4 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.

2.10.12.5 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:

2.10.12.5.1 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.

2.10.12.5.2 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.

2.10.12.5.3 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.

2.10.12.5.4 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.

2.10.12.5.5 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 PSP and procedures.

2.10.12.5.6 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.

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

2.10.12.5.8 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.

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

2.10.13 Mock Adversary Force Member Training and Qualification Process

2.10.13.1 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.

2.10.13.2 The goals of the process are:

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

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

(1) 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.

(2) 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.

(3) 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.

(4) 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.

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

2.10.14 Mock Adversary Force Member Knowledge, Skills, and Abilities

2.10.14.1 As described in Section VI, paragraph C.3.(l)(2) of Appendix B to 10 CFR Part 73, 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.

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

(1) Demonstrate a thorough understanding of DBT weapons, including handheld automatic weapons, incapacitating agents, explosives, and hand-carried equipment, and their capabilities. Demonstrate qualifications 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.

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

(3) 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).

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

(5) Understand the application of the no-play area (to include radiation boundaries), areas described in Section 2.10.6 in Appendix B of this RG, and control measures.

(6) 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.

(7) 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.

(8) Demonstrate the tactical use of drill/exercise equipment and weapons, including their effective range and capabilities (including specialized equipment and weapons).

(9) Understand target identification, acquisition, and engagement by players, including rules of engagement.

(10) 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.

(11) Understand the effectiveness of body armor employed by players and its ballistic protection during the exercise.

(12) Understand the rapid, violent, individual, and small-unit movement, maneuver, and attack characteristics.

(13) 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.

(14) Understand the use, effects, and dispersal characteristics of chemical agents and smoke grenades.

(15) Understand the features of any gas mask being used and its limitations in a stressful environment.

(16) 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).

(17) 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.

(18) Understand the use of MILES equipment.

(19) Understand red gun equipment usage, application, and safety.

(20) 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.

(21) Demonstrate firearms proficiency with all types of weapons that might reasonably be employed during FOF drills or exercises.

(22) Understand the function, design, and capabilities of applicable plant delay systems and delay capabilities and defeat task times.

(23) Understand the use of deadly force.

(24) Understand exercise and site safety procedures including procedures, guidelines and references, and the procedures for the use and control of safeguards information.

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

2.10.14.3.1 The site adversary training program should build upon the following learning objectives:

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

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

2.10.14.3.3 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:

(1) drill timeline coordination (situational awareness and proper cue injects).
(2) cover and concealment assessment.
(3) individual and team tactical movement.
(4) physical security systems and barriers.
(5) any specialized equipment.
(6) MILES equipment usage and safety.
(7) red gun equipment usage and safety.
(8) weapons/explosives capabilities and simulation methods; and
(9) safety control.

2.10.14.3.4 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.

2.10.14.3.5 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.

2.10.15 Conduct of Drills and Exercises

2.10.15.1 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:

(1) 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.

(2) Exercise Participant Safety—The following criteria should be part of the safety briefing for exercise participants:

(a) Physical contact should occur only after a participant has been disabled, surrendered, or neutralized and only with the approval of a controller.

(b) No attempt should be made to disarm an opponent in any way.

(c) All ascents and descents from elevated positions will involve a ladder, stairway, or other safe method.

(d) There should be no jumping from one elevation to another.

(e) All exercise controllers and participants will be briefed on the radiological and industrial safety restrictions and concerns.

(f) Participants should monitor their own condition for overexertion.

(g) 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.

(h) The lead controller should discuss plant and weather conditions before the start of each exercise and address limitations on running, jogging, or walking.

(i) All participants should use personal protective equipment unless otherwise determined by a controller.

(3) 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:

(a) all adversaries are neutralized or have given up the mission.
(b) a complete target set has been destroyed.
(c) 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.
(d) the lead controller determines a condition adverse to personnel or plant safety exists; or
(e) the lead controller directs that the exercise stops.

2.10.15.2 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:

(1) Each participant is personally responsible for his or her safe conduct.

(2) Each participant should monitor his or her condition.

(3) Participants who hear an announcement to stop the exercise should immediately stop all exercise activity and maintain their position until they receive additional instructions.

(4) 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.

(5) 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.

(6) 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.

2.10.15.3 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:

(1) Safety is paramount. The safety of participants, controllers/evaluators, plant personnel, and the plant should never be compromised.

(2) If identifying clothing or items such as armbands are assigned, participants should wear them at all times during the drill or exercise.

(3) Participants will follow all instructions given by a controller.

(4) 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.

(5) If the drill or exercise is temporarily halted, all participants should stop at their locations, cease all firing and movement, and wait for direction.

(6) 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.

(7) 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.

(8) 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.

(9) 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.

(10) 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.

(11) 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).

(12) 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.

(13) Participants should observe the deadly force rules of engagement as authorized by federal or state law and as defined by station policy. In addition, Section 8.13 of RG 5.75, provides further guidance regarding the proper use of force within the force continuum.

(14) 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.

(15) 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.

(16) The MAF and the insider must replicate, as closely as possible, the specific characteristics or requirements detailed in the DBT.

(17) Sufficient time should be allotted for the MAF to gain intelligence information from the insider.

(18) 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.

(19) 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.

(20) 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.

(21) 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.

(22) 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 LE to provide the capability to interdict and neutralize the adversary, the licensee's reliance on LE 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 the LE armed responders to carry out their tactical operations to interdict and neutralize the DBT adversaries. Pursuant to 10 CFR 73.55(b)(10), the licensee shall enter identified drill or exercise deficiencies that adversely affect or decrease the LE 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 LE 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. Alarm station personnel should be evaluated for assessment, communication, coordination, including LE notification/coordination, and other aspects of their operations under contingency events. The LE response team leader should be evaluated for performance in demonstrating command and control and making sound and timely decisions for direction of LE response personnel to interdict and neutralize the DBT threat. Controllers should be evaluated for accurately assessing the individual and overall licensee and LE response to a contingency event.

3.3 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 As described in Section VI, paragraph C.3.(g) of Appendix B to 10 CFR Part 73, each tactical response drill and FOF exercise shall include a documented post-exercise critique in which participants identify failures, deficiencies, or other findings in performance, plans, equipment, and strategies. In accordance with Section VI, paragraph C.3.(i) of Appendix B to 10 CFR Part 73, 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 shall be entered into the licensee's corrective action program to ensure that timely corrections are made to the appropriate program areas.

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

(1) Each position and participant should be evaluated.

(2) The ability of each participant to satisfy the performance criteria associated with his or her position should be evaluated.

(3) Criteria not evaluated should be indicated on the critique. Evaluators should consider using "NE" (not evaluated) instead of "NA" (not applicable).

(4) The form should indicate whether the individual satisfied the performance criteria.

(5) Any issues identified because of the individual's performance should be documented. Issues should be correlated to their respective evaluation standards.

(6) Controller/evaluator performance evaluation comments should be solicited.

(7) The critique material should give participants the opportunity to critique their own actions and to provide feedback on the drill or exercise.

(8) The critique should include an overall assessment of the success of the drill or exercise in meeting the key program elements identified.

(9) Security equipment performance and security system performance should be evaluated as it relates to the licensee's protective strategy.

4.3 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.

(1) 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:

(a) All participants in the drill or exercise are in attendance.

(b) The scenario, including goals and objectives, is thoroughly reviewed with the participants as a group.

(2) 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:

(a) 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.

(b) If a participant took action that resulted in friendly fire, then the participant and controller report should provide specific details of the actions.

(c) 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.

(d) 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.

(e) 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.

(f) During the review of the results, participants should be asked for suggestions for correcting issues and concerns, and these suggestions should be discussed.

(g) 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.

(h) 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 As described in Section VI, paragraphs C.3.(g), (h), and (i), of Appendix B to 10 CFR Part 73, the results of a tactical response drill or FOF exercise shall be documented and entered the licensee's corrective action program. The following information shall be part of the drill or exercise documentation:

(1) Controllers,
(2) MAF,
(3) scenario description,
(4) key elements and evaluation criteria in the drill,
(5) failures, deficiencies, or other findings in performance, plans, equipment, or strategies,
(6) actions taken on failures, deficiencies, or other findings,
(7) 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
(8) 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 Section 5.21.1 of RG 5.75:

(1) date and time,
(2) drill/exercise number or another identifier,
(3) plant conditions, security system status, and weather conditions,
(4) program or process strengths identified, and
(5) 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. As described in Section VI, paragraph C.3.(j) of Appendix B to 10 CFR Part 73, the licensee must protect deficiencies identified during a drill or exercise consistent with the requirements of 10 CFR 73.21.

5.4 The training program normally addresses issues or deficiencies related to training and human performance. As described in Section VI, paragraph C.3.(i), all program element deficiencies shall 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 must be maintained as records. As described in Section VI, paragraph C.3 and H. of Appendix B to 10 CFR Part 73, and 10 CFR 73.55(q), the licensee shall retain the following documents:

(1) scenarios,
(2) participation records showing which security force personnel participated in tactical drills and FOF tactical exercises, and when LE armed responders implementing the LECR participated, records should show which LE armed response personnel participated in the tactical drills and FOF tactical exercises,
(3) completed critique material, including chronologies,
(4) final drill or exercise report, and
(5) resolution or proposed resolution of critique items.

5.6 As described in Section VI, paragraph C.3.(h), of Appendix B to 10 CFR Part 73, the licensee shall retain an attendance roster for all drill- and exercise-related trainings and briefings. Documents that are to be retained as records should be legible and completed appropriately. They must be maintained consistent with NRC regulations, including 10 CFR 73.70, 73.21, and 73.22.

Response Validation Options	Benefits	Challenges/Limitations
Full-Scale Exercise with laser engagement equipment	• Includes elements from the LX 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 LE weapons fire, heat, noise, radiation, interior complexity of site, communications challenges) • Necessitates sound tactical plans and movements • Laser engagement equipment provides the realistic tactical stimuli to which LE team members can respond, instead of responding to verbal information or a written inject. • Can identify potential incidences of fratricide or lessons learned on how to avoid them in the future	• Includes elements from the LX 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 LE 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 LE 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 • 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 to DG 5072
Security Bounding Time and
Adversary Interference Precluded Time

1.0 Applicable Rules and Regulations

10 CFR 73.55(f)(1): *The licensee shall document and maintain the process used to develop and identify target sets, to include the site-specific analyses and methodologies used to determine and group the target set equipment or elements.*

10 CFR 73.55(s)(1)(iv) *Analysis. The applicant or licensee electing to meet one or more of the alternative security requirements in paragraph (s)(2) of this section must perform a technical analysis demonstrating how it meets the criteria in paragraph (s)(1)(ii) of this section. The licensee must maintain the analysis until the certifications required by § 50.82(a)(1) of this chapter or § 52.110(a) of this chapter have been submitted by the licensee.*

10 CFR 73.55(s)(2)(ii)(A)(*2*): *The licensee must provide adequate delay for threats up to and including the DBT of radiological sabotage to enable law enforcement or other offsite armed responders to fulfill the interdiction and neutralization functions for threats up to and including the DBT of radiological sabotage.*

2.0 Security Bounding Time (SBT) Concept

2.1 Licensees should adhere to the guiding principle that an SBT for SMRs or non-LWRs reflects the period of time that would be needed, following the initiation of a hostile action at a nuclear power reactor, for adversary interference to be precluded and for operators to complete actions that would prevent significant offsite release of radionuclides from any source. For an SMR or non-LWR licensee that relies on LE or other offsite personnel (e.g., licensee proprietary or contracted force) to interdict and neutralize the DBT adversary, the licensee should calculate a site-specific SBT as indicated below. Once calculated, a licensee should use the SBT to define

1) the period that the offsite radiological consequences analysis required by 10 CFR 73.55(s)(1)(iv) should consider,
2) the time after which target sets may be screened,[4] and
3) the adversary delay time that its protective strategy should provide if the licensee elects to meet the alternative physical security requirement in 10 CFR 73.55(s)(2)(ii).

2.2 Licensees should consider that responses to their calls for assistance during an attack could have one of two immediate objectives: 1) 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 2) 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 the offsite response force 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

[4] See Regulatory Guide 5.81, Revision 2, for additional information regarding the target set screening process.

of the facility for a subsequent, mutual aid force(s) to interdict and neutralize. Licensees should ensure that offsite response personnel that the licensees rely upon to interdict and neutralize the DBT adversary are prepared for both mission types. For the purpose of SBT, licensees should calculate an SBT for each mission type, and when they differ, implement the longer of the two SBTs.

2.3 Licensees should calculate an SBT by identifying and adding the following six time elements: 1) Alarm Assessment and Communication, 2) Response, 3) Mission Preparedness, 4) Mission Execution, 5) Additional Action, and 6) Safety Margin. Once calculated, a licensee should round its SBT up to the next full hour (e.g., 13¼ hours becomes an SBT of 14 hours). A licensee should recalculate its SBT when any of the elements used to calculate the SBT increase; when any of the elements used to calculate the SBT decrease, a licensee may opt to recalculate its SBT or maintain its original SBT so that it does not have to reassess or revise its target sets, offsite consequence analysis, and adversary delay time.

(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 onsite 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) Additional Action Time[5]	Additional action time is the longest task time for the available preventative or mitigative measures that a licensee could take after loss of a target set and after all known adversaries are neutralized (i.e., applicable only to an adversary-focused mission).

[5] Additional Action Time is a term that staff introduced in Enclosure 2 to SECY 20-0070 (not publicly available), as a necessary component of an acceptable SBT calculation methodology.

(6) 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 SBT.

2.4 Although the SBT calculation methodology uses six discreet time elements, staff 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 six time elements when it calculates an SBT for adversary-focused missions. For plant condition-focused missions, a licensee will not need to identify an Additional Action Time, because the Mission Execution Time will already include the time it takes for site staff to complete preventative or mitigative actions. Another example is 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, essentially condensing the timelines for response and mission preparedness to only the time needed for response. Because the basis and justification for a site-specific SBT could vary significantly from one site to another, a licensee should fully document its SBT development process and decisions and have them available for inspection.

2.5 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 LE 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., 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 the drills or exercises that are required by Appendix B to 10 CFR Part 73, Section VI, paragraph C.3.(l)(1).

3.0 Guidance for Determining the Six SBT Elements

3.1 Alarm Assessment and Communication Time

3.1.1 Alarm Assessment and Communication Time has two components: 1) the maximum time it takes the licensee to detect and assess threats up to and including the DBT, and 2) the maximum time it could take for the licensee to notify the responsible offsite 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 LE or other responsible 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 SBT 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 SBT 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 SBT 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 at a site or the drills or exercises that are required by Appendix B to 10 CFR Part 73, Section VI, paragraph C.3.(l)(1). 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 LE or other offsite armed response personnel, or on planning time data obtained from LE or other offsite armed response personnel for similar emergencies at comparable facilities (i.e., complex industrial environments).

3.3.2 It is unlikely that LE 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). Licensees should ensure that LE 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 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 typically experienced by the LE or other offsite armed responders.

3.3.3 To the extent practical, licensees should replicate real-world conditions during the drills and exercises that are required by Appendix B to 10 CFR Part 73, Section VI, paragraph C.3.(l)(1). For example, 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 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 LE 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, LE or other 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 SBT.

3.3.5 Licensees that want opportunities to periodically establish shorter Mission Preparedness Times and use those times to recalculate their SBTs should use mission preparedness data from the most recent 3-year period. Using data from the past 3 years should 1) result in SBTs that more accurately reflect licensees' and LE or other offsite armed responders' current performance capabilities, and 2) provide the flexibility for licensees to credit shorter Mission Preparedness Times (and by extension shorter SBTs) 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. Licensees should also ensure that the data used to calculate SBTs represent LE 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 SBT 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 SBT calculation. To calculate the 75th percentile, a licensee should use one of these two methods:

Method 1

3.3.6.1 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 (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(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 SBT calculation.

Method 2

3.3.6.2 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 The resulting number is called the 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 75th 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 75th 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 75th 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 SBT 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 75th 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 SBT 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 that are required by Appendix B to 10 CFR Part 73, Section VI, paragraph C.3.(l)(1).

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 LE or other offsite armed response personnel, or on execution time data obtained from LE or other offsite armed response personnel for similar emergencies at comparable facilities (i.e., complex industrial environments).

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 LE 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 LE 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 typically experienced by the LE or other offsite armed responders.

3.4.5 For plant condition-focused missions, Mission Execution Time should include the credible task time for preventative or mitigative actions than 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: 1) offsite armed responders navigating to onsite personnel, escorting them to equipment stored in an owner controlled area, and then reentering the site together with the equipment; 2) offsite armed personnel rendezvousing with recalled offsite licensee personnel and entering the site together with the equipment; 3) offsite armed responders navigating to high ground like the rooftops of protected area buildings so armed responders can use their weapons to cover hose or cable runs in outdoor areas without positioning themselves in the target area; or 4) armed response personnel sweeping, clearing, and holding 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 LE 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, LE 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 SBT.

3.4.7 Licensees that want opportunities to periodically establish shorter Mission Execution Times and use those times to recalculate their SBTs should use mission execution data from the most recent 3-year period. Using data from the past 3 years should 1) result in SBTs that more accurately reflect licensees' and LE or other offsite armed responders' current performance capabilities, and 2) provide the flexibility for licensees to credit shorter Mission Execution Times (and by extension shorter SBTs) as their and LE 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. Licensees should also ensure that the data used to calculate SBTs represent LE 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 SBT 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 75th percentile in its SBT calculation. To calculate the 75th percentile, a licensee should use one of the two methods described in Section 3.3.6.

3.5 Additional Action Time

3.5.1 Additional action time is the longest task time for the available preventative or mitigative measures that a licensee could take after loss of a target set and after all known adversaries are neutralized. Licensees should identify an Additional Action Time only for adversary-focused missions, because the maximum credible task time for preventative or mitigative actions will be included in the Mission Execution Time for plant condition-focused missions. To identify a maximum 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.

3.5.2 Because licensees will likely conduct preventative or mitigative action-related drills or exercises less frequently than security drills and exercises, licensees that want opportunities to periodically establish shorter Additional Action Times and use those times to recalculate their SBTs should use performance data from the most recent 5-year period. Using data from the past 5 years should 1) result in SBTs that more accurately reflect licensees' and LE or other offsite armed responders' current performance capabilities, 2) provide sufficient data for calculating an acceptable Additional Action Time estimate (see paragraph 3.5.3), and 3) provide the flexibility for licensees to credit shorter Additional Action Times (and by extension shorter SBTs) as their and LE or other offsite armed responders' knowledge, training, and performance improves. Licensees should document additional action times from all real-world incidents and drills and exercises. Licensees should also ensure that the data used to calculate SBTs represent their and LE or other offsite armed responders' additional action times for the range of possible preventative or mitigative actions; licensees should not rely on additional action data that, collectively, exclude preventative or mitigative actions from either end of the complexity or time spectrums.

3.5.3 A licensee with fewer than 5 years of data should use the longest documented Additional Action Time in its SBT calculations. After a licensee has documented additional action times for at least 5 years from real-world incidents, drills, or exercises, and for a variety of possible preventative or mitigative actions, the licensee may use an Additional Action Time that represents the 75th percentile in its SBT calculation. To calculate the 75th percentile, a licensee should use one of the two methods described in Section 3.3.6.

3.6 Safety Margin Time

3.6.1 Safety margin time attempts to account for the uncertainties that may exist in the data used to calculate an SBT, or different conditions at the time of an attack than those considered or assumed by a licensee's SBT calculation methodology. Examples of uncertainties include potential inclement weather; chemical, 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.

3.6.2 Prior to a licensee operating a site for at least 10 years, the licensee should use a safety margin of 50% of the total of SBT time elements 2 through 5 (i.e., Response Time, Mission Preparedness Time, Mission Execution Time, and Additional Action Time) for its SBT calculation. After a licensee has been operating a site for at least 10 years, the licensee may use a safety margin of 25% of the total of those same four SBT element times for its SBT calculation.

4.0 SBT Examples

Example 1

4.1 Licensee facility in an urban area

Years in operation: 0 (facility under construction)
Bounding mission: Adversary-focused

SBT Calculation:

Alarm Assessment and Communication Time 1 minute to receive and assess alarm 15 minutes to notify offsite armed responders	16 minutes
Response Time city police tactical team(s) establishes a near-site staging area	1½ hours
Mission Preparedness Time lack of familiarity with facility, adversary, and potential missions	4 hours
Mission Execution Time travel to the site, negotiate delay features, neutralize adversary	2½ hours

Additional Action Time — 3 hours
complete a diverse and flexible coping strategy procedure

Subtotal: 11 hours, 16 minutes
Safety Margin Time (50% of SBT elements 2 through 5) + 5 hours, 30 minutes
1½ + 4 + 2½ + 3 = 11 x .50 = 5½ hours — 16 hours, 46 minutes

SBT = 17 hours (when rounded up to the nearest hour)

Example 2

4.2 . Licensee facility in a rural location

Years in operation: 10 years
Bounding mission: Plant condition-focused

SBT 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

Additional Action Time — 0 minutes
included in Mission Execution Time

Subtotal: 7 hours, 20 minutes
Safety Margin Time (25% of SBT elements 2 thru 5) + 1 hour, 45 minutes
4 + 0 + 3 + 0 = 7 x .25 = 1¾ hours — 9 hours, 5 minutes

SBT = 10 hours (when rounded up to the nearest hour)

5.0 Adversary Interference Precluded Time (AIPT) Concept

5.1 After the initiation of a physical attack, AIPT represents the point at which an SMR or non-LWR licensee can assume that the adversary would no longer interfere with a reactor operator's movement or actions. An SMR or non-LWR licensee can use AIPT during the target set development process to determine when the adversary interference criterion for a credible operator action is satisfied.[6] The AIPT calculation methodology described below is consistent with the alternative method described in Section 5.5.3 of RG 5.81, and it is analogous to how large LWR licensees apply the reasonable assurance of protection time that is described in Section 1.2 of RG 5.76, "Physical Protection Programs at Nuclear Power Reactors" (SGI).

5.2 To calculate AIPT, an SMR or non-LWR licensee should use the following four time elements from their SBT calculations for adversary-focused missions: Response Time, Mission Preparedness Time, Mission Execution Time, and Safety Margin. A licensee does not need to consider an Additional Action Time when calculating an AIPT because the licensee adds the task time for specific mitigative actions (i.e., similar to an Additional Action Time) to the AIPT during the target set development process to determine whether a target set is achievable. Once calculated, a licensee should round its AIPT up to the next full hour (e.g., 11¼ hours becomes an AIPT of 12 hours). A licensee should recalculate its AIPT when any of the elements used to calculate the AIPT increase; when any of the elements used to calculate the AIPT decrease, a licensee may maintain its original AIPT so that it does not have to reassess or revise its target sets.

5.3 Prior to a licensee operating a site for at least 10 years, the licensee should use a safety margin of 50% of the total of SBT time for elements 2 through 4 (i.e., Response Time, Mission Preparedness Time, and Mission Execution Time) for its AIPT calculation. During the 10 year period, the licensee would perform its annual and quarterly drills and exercises and complete three triennial force-on-force NRC-graded exercises. These drills and exercises should enable the licensee to obtain sufficient experience with performance of the contingency response strategy and effectively implement corrective actions to address any identified deficiencies. Based upon the anticipated level of experience and maturity of the licensee's security programs, after 10 years of operation the licensee may use a safety margin of 25% of the total of those same three SBT element times for its AIPT calculation.

5.4 Example 1 above reflects an SBT based on an adversary-focused mission. The AIPT for the hypothetical site that is under construction in Example 1 would be:

Alarm Assessment and Communication Time	16 minutes
Response Time	1½ hours
Mission Preparedness Time	4 hours
Mission Execution Time	+2½ hours
Subtotal:	8 hours, 16 minutes

Safety Margin Time (50% of SBT elements 2 thru 4) + 4 hours, 0 minutes

1½ + 4 + 2½ = 8 x .50

= 4 hours 12

hours and 16 minutes

6 For additional information regarding credible operator actions and the adversary interference criteria refer to Section 5.5 in Regulatory Guide 5.81.

Appendix C to DG 5072
Security Bounding Time and
Adversary Interference Precluded Time

AIPT = 13 hours (when rounded up to the nearest hour)

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.
10. NRC, SECY 20-0070, "Technical Evaluation of the Security Bounding Time Concept for Operating Nuclear Power Plants," July 30, 2020, (ML20126G332).

REFERENCES[7]

1 *U.S. Code of Federal Regulations* (CFR), "Definitions," Part 171.5, Chapter 1, Title 10, "Energy."

2 CFR, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," Part 73.55, Chapter 1, Title 10, "Energy."

3 CFR, "Physical Protection of Plants and Materials," Part 53, Chapter 1, Title 10, "Energy."

4 CFR, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter 1, Title 10, "Energy."

5 CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter 1, Title 10, "Energy."

6 U.S. Nuclear Regulatory Commission (NRC), Regulatory Guide (RG) 1.145, "Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants," Washington, DC.

7 NRC, RG 1.183, "Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors," Washington, DC.

8 NRC, RG 1.194, "Atmospheric Relative Concentrations for Control Room Radiological Habitability Assessments at Nuclear Power Plants," Washington, DC.

9 NRC, RG 1.233, "Guidance for a Technology-Inclusive. Rick-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," Washington, DC.

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

11 NRC, RG 5.71, "Cyber Security Programs for Nuclear Facilities," Washington, DC.

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

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

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

15 NRC, RG 5.77, "Insider Mitigation Program," Washington, DC. (not publicly available)

---

[7] Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site 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 on line or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov.

Copies of International Atomic Energy Agency (IAEA) documents may be obtained through their Web site: 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 E-Mail at Official.Mail@IAEA.Org

16 NRC, RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors," Washington, DC. (not publicly available)

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

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

19 NRC, NUREG 1964, "Access Control Systems: Technical Information," Washington, DC.

20 NRC, NUREG/CR 7201, "Characterizing Explosive Effects on Underground Structure," Washington, DC.

21 NRC, NUREG/CR 6190, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants: Vehicle Barrier System Siting Guidance for Blast Protection," Vols. 1 and 2, Washington, DC.

22 U.S. Department of Energy, Sandia National Laboratory, "Access Delay Technology," SAND99-2168.

23 U.S. Department of Energy, Sandia National Laboratory, "Vital Area Identification for U.S. Regulatory Nuclear Power Reactor Licensees and New Reactor Applicants," SAND2008-5644.

24 U.S. Department of Energy, Sandia National Laboratory, "Security Assessment Technical Manual," SAND2007-5591.

25 Atomic Energy Act of 1954, as amended, Section 42, United States Code (U.S.C.).

26 Federal Register (FR) Notice, "Nuclear Regulatory Commission International Policy Statement" (79 FR 39415), July 10, 2014.

27 Management Directive and Handbook 6.6, "Regulatory Guides," Washington, DC.

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

29 IAEA Nuclear Security Series No. 27-G, "Physical Protection of Nuclear Material and Nuclear Facilities (implementation of INFCIRC/225/Revision 5)"

30 Management Directive and Handbook 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," Washington, DC.